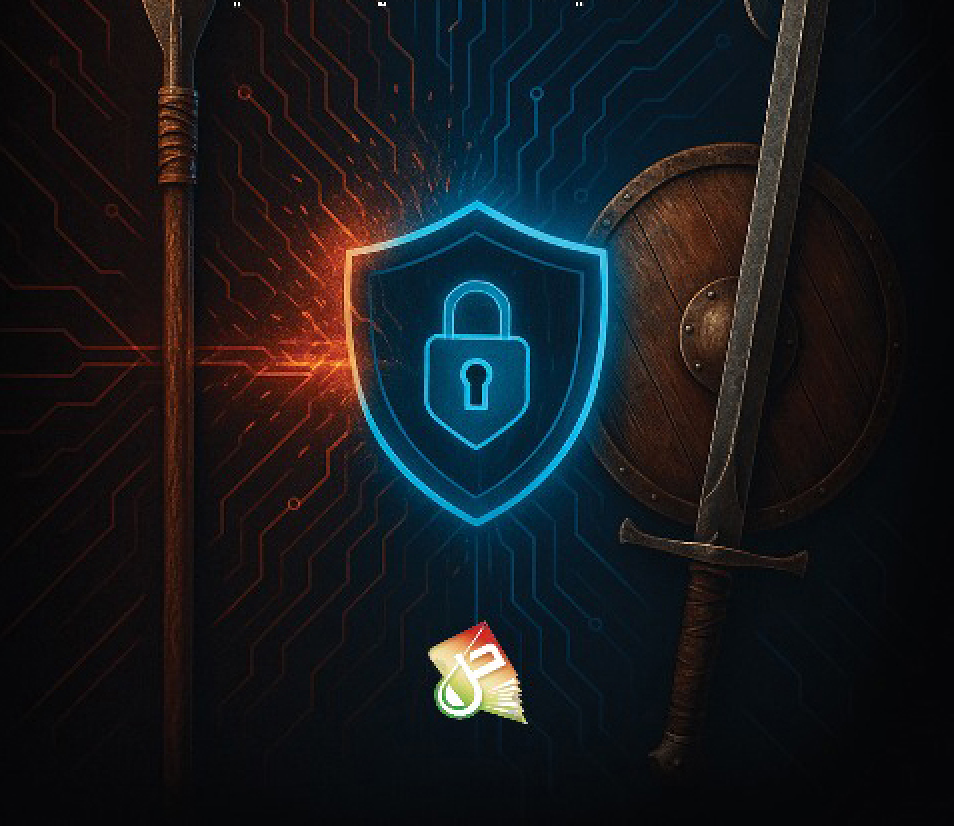
# السيادة الرقمية
## وهندسة القرار
## في الأمن السيبراني المتقدم

الدكتورة
**رشا إبراهيم الفواعير**
مدربة وباحثة في مجال الأمن السيبراني والتحول الرقمي



بسم الله الرحمن الرحيم

﴿ وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ۖ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ ﴾

صدق الله العظيم

**السيادة الرقمية وهندسة القرار في**

**الأمن السيبراني المتقدم**

# السيادة الرقمية وهندسة القرار
# في الأمن السيبراني المتقدم

الدكتورة

**رشا إبراهيم الفواعير**

**الطبعة الأولى**

2026م – 1447هـ

**دار صفاء للطباعة والنشر والتوزيع - عمان**

دار صفاء للطباعة والنشر والتوزيع

عنوان الكتاب :السيادة الرقمية وهندسة القرار في الأمن السيبراني المتقدم

تأليف : الفواعير . رشا ابراهيم

رقم التصنيف : 005.8

الواصفات : الأمن السيبراني //التغير التكنولوجي //أمن البيانات//الهيمنة//أتخاذ القرارات//الذكاء الاصطناعي//

رقم الإيداع لدى دائرة المكتبة الوطنية( 2025/9/5244 )

ISBN 978-9923-28-388-2 ردمك

عمان – شارع الملك حسين

مجمع الفحيص التجاري- تلفاكس–4612190 6 962+

هاتف– 4611169 6 962+ ص . ب922762 عمان–11192 الأردن

DAR SAFA Publishing - Distributing

Telefax: +962 6 4612190- Tel: + 962 6 4611169

P.O.Box: 922762 Amman 11192- Jordan

E-mail:safa@darsafa1.net

E-mail:safa@darsafa.info

www.darsafa.net

# الاهداء.....

إلى المجتمع الأكاديمي والمهني،
إلى كل باحث يسعى إلى الحقيقة، وصانع قرار يتطلع إلى أدوات المستقبل،
وإلى كل طالب علم يؤمن أن السيادة تبدأ من امتلاك المعرفة...

إليك يا حمزة، أيقونة الغياب الحاضر، ومصدر الإلهام الذي حول الفقد إلى قوة، والوجع إلى رسالة.

أهدي هذا الكتاب بوصفه جهدا علميا ومعرفيا يربط النظرية بالتطبيق، ويحول الأمن السيبراني من إطار تقني ضيق إلى قدرة سيادية وطنية ومنظور استراتيجي شامل.

إنه ليس مجرد فصول تقرأ، بل دعوة للتفكير والعمل، ومنصة لتبادل الخبرات، وخارطة طريق عملية ترشد إلى بناء فضاء رقمي آمن، مرن، ومستدام... سيادة وفكرا ومستقبلا.

# عن المؤلف

الدكتورة المهندسة **رشا إبراهيم الفواعير**، مدربة وباحثة ومختصة في إدارة الأمن السيبراني، وخبيرة لأكثر من 18 عامًا في هندسة الحاسوب والتحول الرقمي وإدارة نظم المعلومات الجغرافية. تولّت مناصب قيادية في بلدية السلط الكبرى، وعُرفت بقدرتها على الدمج بين الفكر الأكاديمي والخبرة العملية.

هي صاحبة مبادرة **"درعك الرقمي – سيبر آمن"**، المبادرة المجتمعية الرائدة التي أُطلقت برعاية بلدية السلط الكبرى، وتهدف إلى نشر الوعي السيبراني عبر محاضرات وكورسات تدريبية موجهة لبناء جيل أكثر أمانًا في العالم الرقمي.

يأتي هذا الكتاب ليجسّد مسيرة المؤلف بين العلم والتطبيق، وليفتح للقارئ نافذة على عالم الأمن السيبراني، بأسلوب يجمع بين العمق والفائدة والإلهام.

# رسالة إلى المقام السامي......

**إلى مقام حضرة صاحب الجلالة الهاشمية الملك عبد الله الثاني ابن الحسين المعظّم وإلى صاحب السمو الملكي وليّ العهد الأمير الحسين بن عبد الله الثاني، حفظهما الله**

**السلام عليكم ورحمة الله وبركاته،**

**الموضوع :نحو سيادةٍ رقميةٍ فاعلة**

يصــدر هذا الكتاب في زمنٍ تتبدّل فيه موازين القوة من حدودٍ تُحرس بالجيوش إلى فضـاءاتٍ تُصـان بالبيانات والخوارزميات. وفي صـميم هذا التحوّل تقف السـيادة الرقمية مكوّنًا سياديًا يعيد تعريف استقلال الدولة وأمنها وازدهارها. يضع هذا العمل بين أيديكم خارطة طريق تنفيذية مكثّفة (90 يومًا) تحوِّل الأمن السيبراني من ردّ فعلٍ متأخر إلى قرارٍ سياديٍّ استباقي يُدار بمنهجية واضحة ويُقاس بمؤشرات أداء دقيقة.

لقد اسس الأردن قاعدة صلبة تستحق البناء عليها، مثل تأسيس المركز الوطني للأمن السـيبراني، وفريق JoCERT، واسـتراتيجيات وطنية متعاقبة، وبرامج أكاديمية تُنمّي رأس المال البشري. غير أنّ سرعة التحوّل العالمي تقتضي قفزة نوعية تُوحِّد الجهود في غرفة قرار وطنية مرتبطة لحظيـًا بالقطاعات الحيوية، ومركز إنذار مبكر، وإطارٍ موحَّدٍ للاستجابة، ولوحة مؤشـرات سيادية تنقل الخطاب من العموميات إلى أرقام تُدار وتُراجع.

**وعد الكتاب**

أن نقدّم لصــانع القرار الأردني خطة تشــغيلية قابلة للتنفيذ خلال 90 يومًا تقوم على منهجية:

رصـــد – تحليل – قرار – تنفيذ – مراجعة، مصـــحوبة بقوائم تحقق، ومصـــفوفات مخاطر، وتمارين محاكاة(Red vs Blue) ، ونماذج تقارير ولوحة مؤشرات (KPIs) لقياس زمن الاكتشاف والاستجابة، وتقليص الخسائر، وتعزيز الثقة العامة.

**خطوات نلتمس لها الرعاية السامية**

1. إشـــهار «الميثاق الســـيادي الرقمي الأردني «برعاية ملكية ســـامية إطارًا ناظمًا للمبادئ والالتزامات عبر القطاعات.
2. تشكيل مجلس توجيه سيبراني وبدء تجربة وطنية لمدة 90 يومًا تُشغَّل فيها غرفة القرار بكامل طاقتها وتُنظَّم تمارين محاكاة قطاعية.
3. تفويض إنشـــاء وتشـــغيل غرفة القرار الســـيادي الوطنية (24/7) وربطها تقنيًا وقانونيًا بقطاعات الطاقة والمال والاتصالات والصحة والنقل.
4. اعتماد الإطار الوطني الموحّد للاستجابة للحوادث مع نشـر موجز ربع سنوي لمؤشـرات الأداء :زمن الاكتشـاف/ الاسـتجابة، الخسـائر المُخفَّضـة، مستوى الثقة العامة.
5. إطلاق منصـــة شـــراكة وطنية (حكومة—قطاع خاص—جامعات) وبرنامج زمالة سيبرانية وطنية للشباب، إلى جانب سياسات مشتريات ومعايير مفتوحة تقلّل الارتهان التقني وتُنمّي القدرات المحلية.

**تعهّد المؤلف**

هذا الكتاب أداة للتنفيذ لا نصًّـــا للقراءة فقط. نلتزم بدعم التطبيق تدريبًا واســـتشـــارةً وإعدادًا للقوالب التشغيلية وقياسًا للأثر، وتحديث المنهجية بما يوافق الخصوصية الأردنية ويحفظ الحقوق والخصوصية وسيادة القانون.

ختامًا، إنّ الأردن بقيادتكم الحكيمة، وموقعه الرابط، وتنوعه المجتمعي، ورأسماله البشري الشاب، قادرٌ على الانتقال من موقع المتلقّي إلى موقع صانع الرؤية إقليميًا. وحين تلتقي الإرادة السياسية بالبنية المؤسسية والقدرة التنفيذية، تتحوّل السيادة الرقمية من شعارٍ مُعلَّق إلى قدرة دولة تُقاس وتُدار.

حفظكم الله ورعاكم،والسلام عليكم ورحمة الله وبركاته.

# المحتويات

**الفصل الثالث**

**هندسة القرار السيبراني**

**المفهوم والأدوات**



**الفصل الرابع**

**الذكاء الاصطناعي في مواجهة التهديدات السيبرانية**

**الفصل الخامس**

**السيادة الرقمية بين السياسة والتكنولوجيا**



**الفصل السادس**

**الأمن السيبراني في البنى التحتية الوطنية**

## الفصل السابع

## بناء منظومات قرار سيادية متكاملة

**الفصل الثامن**

**السيادة الرقمية بين التحول العالمي والتجربة الأردنية**

**من التحديات الكونية إلى النماذج الوطنية**



**الفصل التاسع**

**دروس مستخلصة من الميدان السيبراني**

# افتتاحية الكتاب

"إذا عرَفت نفسك وعرَفت عدوك، فلن تخشى مائة معركة — "سن تزو، فن الحرب.

بهذه الحكمة القديمة تبدأ القصة الجديدة. معركة اليوم ليست على تخوم المدن، ولا في صحراء مفتوحة، بل في فضاءٍ غير مرئي، تصنعه الخوارزميات وتُخاض فيه الحروب بلا جيوش ولا مدافع.

لنتخيّل أن محطات الكهرباء تنطفئ فجأة، وأن شبكات الاتصالات تتوقف بلا سبب، وأن منصات الدفع المالي تتعطل في لحظة حرجة. لم يقتحم العدو حدودًا، ولم يرفع علمًا فوق أرضك، ومع ذلك بات قرارك الوطني مُعطلاً. هنا يتجسّد قول مكيافيلي" :من يؤسس سلطته بالاعتماد على قوة خارجية، لا يملك إلا الوهم".

لقد تغيّر ميدان القوة. لم تعد السيادة تُقاس بمدى امتداد الأرض، بل بمدى السيطرة على البيانات. لم يعد السلاح في البر والجو والبحر، بل في كودٍ رقمي ينساب في شبكاتك، يغيّر الأولويات دون أن تدري. إنّها "حروب بلا دماء"، لكنها أشد فتكًا لأنها تزرع الهزيمة في وعي المجتمع قبل أن تُحدث الدمار في بنيته التحتية.

إنّ دروس الحروب القديمة ما زالت صالحة، لكن ميدانها تبدّل:

- قال سن تزو" :الهجوم هو سر الدفاع؛ والدفاع هو خطة للهجوم ".وهكذا بات الأمن السيبراني الحديث يقوم على الدفاع متعدد الطبقات Defense)

in Depth)، الذي لا يكتفي بالتحصــين، بل يتحوّل إلى هجوم اســتباقي عبر الرصد والتحليل.

- وقال مكيافيلي" :الأمير الحكيم هو الذي يبني على ما يملك، لا على ما يســتعيره ".وهـذا جوهر الســيادة الرقميـة؛ أن تمتلـك بنيتـك الرقميـة، خوارزمياتك، وتشريعاتك، لا أن تستعيرها من آخرين.
- وكتب كلاوزفيتز" :الحرب استمرار للسياسة بوسائل أخرى ".واليوم يمكننا أن نقول :الهجوم السيبراني استمرار للصـراع بوسـائل رقمية، لا تقل خطرًا عن أي مواجهة عسكرية.

إنّ هذا الكتاب لا يروي قصــة خيالية، بل يقدّم قراءة علمية لمســارٍ تحوّلت فيه الحروب من ميادين الجغرافيا إلى فضاءات السيبر. إنه دعوة لتجاوز مرحلة رد الفعل المتأخر، إلى هندســة قرار ســيادي يســتند إلى الرصــد والتحليل والتنبؤ، ثم التنفيذ والمراجعة.

فالسيادة الرقمية لم تعد ترفًا، بل شرطًا وجوديًا للدول. ومن لا يُدرك هذه الحقيقة يجد نفسه أسيرًا لواقع يُدار من خارج حدوده، حتى لو بدت أرضه محمية. إنها معركة جديدة، لكن أصــداء نصــائح ســن تزو ومكيافيلي وكلاوزفيتز ما زالت تتردّد فيها : اعرف نفسك، امتلك أدواتك، وكن سيد قرارك... وإلا صنع غيرك مستقبلك بالنيابة عنك.

# توصيات الكاتب

الكتاب يطرح رؤية استراتيجية متكاملة تؤكد أن الأمن السيبراني لم يعد مجرد أداة تقنية للدفاع، بل تحوّل إلى بُعد سيادي وقرار وطني يُحدد استقلال الدول وقدرتها على البقاء في عصرٍ تُدار فيه القوة عبر البيانات والخوارزميات.

ينطلق من فرضية جوهرية:

أن امتلاك السيادة الرقمية يعني امتلاك القرار، وأن غيابها يضع الدول في تبعية خفية حتى لو بدت أنظمتها محمية تقنيًا.

ولهذا، يقترح الكتاب:

- هندسة منظومة قرار سيادي تقوم على دورة: رصد ← تحليل ← قرار ← تنفيذ ← مراجعة.
- ربط الأمن السيبراني بالأطر العالمية (NIST, ISO/IEC 27001, SAMA) وتطويعها لواقعنا المحلي.
- بناء "غرفة قرار وطنية" قادرة على إدارة الحوادث لحظيًا، وتحويل البيانات إلى قرارات قابلة للقياس.
- دمج البعد التقني مع البعد الفلسفي–السياسي للسيادة، بحيث يصبح الأمن الرقمي أداة لحماية الهوية والاستقلال، لا مجرد استجابة للهجمات.

باختصار:

**الكتاب يقدّم خارطة طريق عملية لتحويل الأمن السـيبراني من رد فعل متأخر إلى قدرة سيادية استباقية تُدار بوعي وقرار، خلال 90 يومًا.**

# عن الكتاب

يقدّم هذا الكتاب خارطةً عملية تجمع بين السيادة الرقمية وهندسة القرار في الأمن السيبراني المتقدم، من الأطر العالميةNIST) ، (ISO/IEC 27001إلى أدوات الذكاء الاصطناعي ودراسات حالة قابلة للتطبيق. إنه مزجٌ ذكي بين النظرية الرصينة والتطبيقات التشغيلية، مصاغ خصيصًا لواقعنا العربي مع إضاءة خاصة على التجربة الأردنية بوصفها نموذجًا واقعيًا يمكن البناء عليه وتعميمه إقليميًا.

بعيدًا عن الإطناب الأكاديمي، يضعك الكتاب داخل خطّ إنتاج القرار السيادي : كيف تُحوِّل البيانات إلى بصيرة، والبصيرة إلى قرار، والقرار إلى تنفيذ يُقاس ويُراجع. ستسير مع خطة مضغوطة من 90يومًا تُحوِّل الأمن السيبراني من رد فعل متأخر إلى قدرة دولة استباقية :تشكيل فريق وطني متعدد التخصصات، رسم خريطة مخاطر قطاعية، تشغيل غرفة قرار سيادي، إنشاء قدرات إنذار مبكر، تنفيذ تمارين Red vs Blue، واعتماد إطار وطني موحّد للاستجابة للحوادث مقرونًا بلوحة مؤشرات أداء.(KPIs)

**لماذا هذا الكتاب الآن؟**

- لأن موازين القوة تُعاد صياغتها في فضاءات البيانات والخوارزميات، لا عند الحدود والجيوش.
- لأن المؤسسات العربية—حكومية وخاصة—تحتاج دليل تشغيل واضحًا لا شعارات عامة.
- لأن الفرصة سانحة لبناء نماذج وطنية للسيادة الرقمية تستند إلى قدرات محلية وشراكات ذكية.

**ماذا سيعطيك الكتاب؟؟**

- خارطة طريق 90 يومًا بتسلسل واضح: (رصد → تحليل → قرار → تنفيذ → مراجعة).
- قوالب جاهزة :مصفوفات مخاطر، سياسات قطاعية، خطط استجابة، تقارير تنفيذية، ونماذج تقييم نضج.
- عدّة محاكاة :سيناريوهات هجومية/ دفاعية (Red vs Blue) قابلة للتكييف لقطاعات الطاقة، المال، والاتصالات.
- لوحة مؤشرات عملية (KPIs) لقياس سرعة الاستجابة، تقليص الخسائر، ورفع ثقة الجمهور.
- دراسات حالة مختصرة تُظهر كيف تُحوَّل المبادئ إلى إجراءات، وكيف تُدار الشراكات بين الحكومة والقطاع الخاص والجامعات.

**لمن نكتب؟**

- صنّاع القرار :وزارات، هيئات تنظيم، قيادات أمنية وخدمية.
- قادة التقنية والأمن :(CISO/CIO/SOC) من يريدون تحويل الامتثال إلى جاهزية تشغيلية.
- المشرّعون وواضعو السياسات :من يسعون لموازنة الأمن والحقوق ضمن أطر مرنة قابلة للتنفيذ.

# وعدٌ للقارئ

ستتعلّم، خطوةً بخطوة، كيف تبني منظومة قرار سيادي قابلة للتنفيذ خلال 90 يومًا. ليست وعودًا نظرية، بل خطوات قابلة للتطبيق اليوم: من أول اجتماع للفريق الوطني، إلى أول تقرير سيادي، إلى أول تمرين محاكاة ناجح، وصولًا إلى تشغيل غرفة القرار وبدء دورة تحسين مستمرة.

افتح هذا الكتاب كما لو أنه اليوم الأول من التسعين—ضع الخطة على الطاولة، افعل الشيء الصحيح التالي، وابدأ العبور من التبعية الرقمية إلى السيادة الرقمية الفاعلة.

**جسور التناغم...**

**"يمثل هذا المؤلف امتدادًا لرؤيتي الأكاديمية والمهنية في بناء فضاء رقمي آمن قائم على المعرفة والوعي. أكتب هنا من موقع الباحثة والخبيرة التي ترى في الأمن السيبراني أكثر من كونه إجراءات تقنية، بل هو ركيزة استراتيجية لحماية الأفراد والمؤسسات والدول.**

**وفي الوقت نفسه، فإن تجربتي في الكتابة في مجال التنمية الذاتية تكشف عن قناعة راسخة بأن حماية الإنسان تبدأ من داخله، من وعيه وقوته النفسية والوجدانية.**

**بهذا التلاقي، تتجسد رسالتي: أن أمن البيانات وأمن الإنسان كلاهما ضرورة لبناء مستقبل متوازن، آمن، ومستدام."**

# المقدمة

امتدت مفاهيم السيادة لتشمل الفضاء السيبراني باعتباره ساحة جديدة للصراع والتنافس بين الدول. وهنا برزت السيادة الرقمية كركيزة جوهرية لاستقلال القرار الوطني وحماية المصالح العليا، في بيئة لا تعترف بالحدود التقليدية. ومن هذا المنطلق، أصبح الأمن السيبراني المتقدم ضرورة استراتيجية، وحجر الزاوية في بناء منظومات دفاع رقمية قادرة على التكيف مع تهديدات معقدة ومتجددة.

يقدّم هذا الكتاب دراسة معمقة في ميدان السيادة الرقمية وهندسة القرار ضمن سياق الأمن السيبراني، جامعًا بين التحليل النظري الرصين والتطبيقات العملية المعاصرة. ويتناول الأطر المفاهيمية والسياسات الاستراتيجية التي تؤسس لحماية فعّالة للفضاء الرقمي الوطني، مع إضاءة خاصة على دور هندسة القرار بوصفها أداة فكرية وتنفيذية لتحويل البيانات إلى قرارات سيادية متزنة.

كما يستند العمل إلى أحدث المراجع والمعايير الدولية مثل NIST Cybersecurity Frameworkو ISO/IEC 27001، إلى جانب الأطر الإقليمية كإطار SAMA، ليضع القارئ أمام رؤية متكاملة للتعامل مع التحديات التقنية، الاقتصادية، والسياسية. ويعرض نماذج هندسية متقدمة، وأدوات الذكاء الاصطناعي والتعلم الآلي، بما يسهم في رفع كفاءة الكشف المبكر، وتسريع الاستجابة، وتعزيز قدرات التصدي للهجمات السيبرانية.

ولا يغفل الكتاب الأبعاد الأخلاقية والتشريعية لحماية البيانات والخصوصية الرقمية، ويستعرض نماذج للتعاون الدولي الرشيد، إلى جانب دراسات حالة عملية

تكشف كيف أسهمت هندسة القرار في تعزيز قدرات الأمن السيبراني على مستوى المؤسسات والدول.

إنه ليس مجرد مرجع تقني أو تنظيري، بل دليل استراتيجي متكامل للباحثين والأكاديميين وصنّاع القرار، يهدف إلى ترسيخ فهم عميق لمفاهيم السيادة الرقمية، وتسخير أدوات هندسة القرار لبناء فضاء سيبراني آمن ومرن وذي سيادة. ففي زمن لم تَعُد فيه القوة تُقاس بالسلاح، بل تُمارس عبر الخوارزميات والشيفرات، يضع هذا الكتاب بين يدي القارئ مفاتيح المستقبل.

# الفصل الأول

# الأمن السيبراني المتقدم

# (المفاهيم والأسس العلمية)

# مقدمة الفصل

أصبح الأمن السيبراني في عصر التحولات الرقمية المتسارعة ركيزة استراتيجية لحماية المؤسسات والدول، ولم يَعُد مجرّد وسيلة تقنية تُستخدم عند الحاجة. فالهجمات السيبرانية اليوم لا تُقاس فقط بتكلفتها الفنية، بل بقدرتها على التأثير في الاقتصاد، والسياسة، والبنى التحتية الحيوية، لتغدو مسألة وجود وسيادة.

يسعى هذا الفصل إلى بناء قاعدة معرفية متينة، تعيد تعريف المفاهيم المركزية مثل: التهديد السيبراني، الثغرة الأمنية، والمخاطر الرقمية، باعتبارها مدخلًا لفهم طبيعة التحديات المعاصرة. كما تقدّم مقارنة بين النماذج الأمنية التقليدية والحديثة، مثل:

- Zero Trust
- Defense in Depth
- Adaptive Security

**وتتعمق في نموذج الحماية الثلاثية – (Confidentiality – Integrity – Availability)** بوصفه إطارًا مرجعيًا شاملاً، إضافة إلى تحليل أبرز التهديدات الحديثة مثل هجمات سلاسل التوريد، وهجمات الفدية، والهندسة الاجتماعية المدعومة بالذكاء الاصطناعي.

يهدف هذا الفصل إلى إرساء قناعة واضحة بأن الأمن السيبراني يبدأ من العقلية والثقافة الأمنية قبل أن يكون مجرد منظومة أدوات، وأن المؤسسات القادرة على التعلم والتكيف هي الأقدر على حماية هويتها وصيانة قرارها في عالم متغير باستمرار.

يعرّف هذا الفصل القارئ بجوهر الأمن السيبراني الحديث، من المفاهيم الأساسية وحتى النماذج المتقدمة مثل Zero Trust و .Defense in Depthيوضح التحول من الأمن التقليدي إلى الأمن التكيّفي والاستباقي، ويضع إطارًا علميًا لفهم التهديدات المعاصرة كأساس لبقية الفصول.

## 1.1 المجالات الحيوية للأمن السيبراني

لم تَعُد المعلومة حبيسة الورق ولا العلاقات مقتصرة على الحضور المادي، بل أصبح الإنسان يعيش في فضاء رقمي شامل يمتد من تفاصيله اليومية إلى قراراته المصيرية المرتبطة بالهوية والسيادة. هذا العالم، رغم ما يحمله من فرص، يزخر بتهديدات ومخاطر متزايدة، ما جعل **الأمن السيبراني** منظومة فكرية واستراتيجية لا تقتصر على التقنية وحدها، بل تُعنى بحماية الإنسان في صورته الرقمية وصون بياناته التي باتت أغلى من الموارد المادية.

**الأمن السيبراني** هو مجموعة من السياسات، الإجراءات، والتقنيات التي تهدف إلى حماية الأنظمة الرقمية، الشبكات، والبيانات من الهجمات والتهديدات الإلكترونية. يشمل الأمن السيبراني مختلف المستويات بدءًا من حماية الأجهزة الشخصية، مرورًا بحماية الشبكات والتطبيقات، وصولًا إلى تأمين البيانات المخزنة في السحابات الرقمية. يُعتبر الهدف الأساسي له ضمان سرية المعلومات، والحفاظ على سلامتها، وضمان توافرها فقط للأطراف المخولة.

1. **أمن الشبكات**: يشكّل خط الدفاع الأول في العالم الرقمي، إذ يحمي البيانات أثناء انتقالها باستخدام الجدران النارية، أنظمة كشف التسلل، والتشفير. إنه

تجسـيد لفكرة جوهرية مفادها أن **الثقة في الفضـاء السـيبراني لا تُمنح، بل تُبنى بعناية.**

2. **أمن التطبيقات**: ينظر إلى البرمجيات ككائنات حية تنبض داخل المنظومات الرقمية، يحمل كل سـطر برمجي فيها احتمالًا لثغرة. لذا يركّز على التصـميم الآمن، والفحص المستمر، وسدّ نقاط الضعف قبل أن تتحول إلى منافذ تهديد.

3. **الأمن السـحابي**: يحمي البيانات الموزعة على منصـات تتجاوز الحدود الجغرافية، من خلال التشفير، وإدارة الهوية، ومراقبة الوصول. وهنا يظهر سؤال جوهري :**في عصـر السـحابة، هل ما زالت بياناتنا ملكًا لنا أم أصـبحت جزءًا من فضاء مشترك؟**

4. **أمن إنترنـت الأشـياء**:(IoT Security) يتعامل مع تحديات الأجهزة الذكية المتصـلة، حيث يُقاس الخطر لا بحجم الجهاز، بل بموقعه داخل المنظومة. يعتمد هذا الأمن على التحقق من الهوية، العزل الوقائي، التحديثات الدورية، والمراقبة السلوكية المستمرة.

5. **أمن البيانات**: يشـكّل القلب النابض للأمن السـيبراني، إذ يصـون المعلومة في مراحلها كافة: التخزين، النقل، والمعالجة. ويعتمد على التشـفير، وضـبط الوصـول، وإدارة دورة حياة البيانات. لأن **من يملك البيانات لا يملك القوة فقط، بل يحمل أيضًا عبء المسؤولية الأخلاقية والمعرفية.**

بهذا المعنى، لا يُختزل الأمن السـيبراني في أدوات أو أنظمة، بل يُفهم كمنظومة فكرية وتقنية تسعى إلى تحقيق **توازن دائم بين الحماية والحرية، وبين الثقة والشـك، وبين الإنسان والآلة.**

## 1.2 أمن البيانات – جوهر الحماية الرقمية

في العالم الرقمي المتسع بلا حدود، لم تَعُد البيانات مجرد أرقام أو ملفات، بل أصبحت الامتداد الرقمي للإنسان، والعصب الاستراتيجي للمؤسسات، وأساس القرارات الوطنية. كل تفاعل يولّد بيانات، وكل قرار يُسجَّل، ما جعل من أمن البيانات قضية سيادة وهوية وثقة، لا مجرد مسألة تقنية.

**أمن البيانات** هو مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى **حماية البيانات** من الوصول غير المصرح به، والتعديل، والسرقة، والتلف، والفقدان. يُعتبر **أمن البيانات** جزءًا أساسيًا من **الأمن السيبراني**، حيث يُركز بشكل خاص على الحفاظ على **سرية** و**سلامة** و**توافر** البيانات عبر جميع مراحل حياتها (التخزين، النقل، والمعالجة).

**يشمل أمن البيانات عدة جوانب مهمة:**

1. **التشفير** :لضمان أن البيانات تكون **غير قابلة للقراءة** إلا من قبل الأطراف المصرح لها.
2. **التحكم في الوصول** :تحديد من يمكنه الوصول إلى البيانات بناءً على **الأذونات** الممنوحة.
3. **النسخ الاحتياطي** :لضمان أن البيانات يمكن استعادتها في حال حدوث فقدان أو تدمير.
4. **إدارة دورة حياة البيانات** :من اللحظة التي يتم فيها جمع البيانات حتى إتلافها بشكل آمن عندما تصبح غير ضرورية.

5. **التصنيف** :تصنيف البيانات وفقًا لمستوى حساسيتها لضمان معالجتها بشكل مناسب.

أمن البيانات ليس مقتصرًا على الحماية التقنية فقط، بل يشمل أيضًا الأبعاد القانونية والأخلاقية، مثل الحفاظ على خصوصية الأفراد وحمايتهم من التسريب أو الاستغلال غير المشروع لمعلوماتهم الشخصية.

### 1.3 حماية البيانات عبر دورة حياتها

حماية البيانات ليست حدثًا منفصلًا يبدأ عند التخزين أو ينتهي بالتشفير، بل هي **رحلة أمنية متصلة** تبدأ من لحظة التكوين وحتى الإتلاف الآمن. تمر البيانات خلال هذه الدورة بمراحل مختلفة، كل منها يمثل بيئة خاصة بخطر محدد ويتطلب سياسة مخصصة:

1. **مرحلة الإنشاء** :تمثل أصل الثقة، إذ إن إدخال معلومة خاطئة أو خبيثة يُفسد كل ما يُبنى عليها. لذا تُستخدم واجهات آمنة، أنظمة تحقق، وفلترة دقيقة للمدخلات.

2. **مرحلة النقل** :البيانات هنا كرسائل تعبر طرقًا عامة، مهددة بالقراءة أو التلاعب. تُحمى عبر تشفير النقل (TLS) وضمان سلامة البيانات أثناء الانتقال.

3. **مرحلة المعالجة** :أكثر المراحل حساسية، حيث تُبنى القرارات. أي ثغرة في بيئات التشغيل أو ضعف في الصلاحيات قد يكشف معلومات حرجة. تُواجه بالعزل الأمني، المراقبة السلوكية، واكتشاف الأنشطة الشاذة.

4. **مرحلة التخزين** :بمثابة الأرشيف الرقمي. التخزين دون تشفير أو ضوابط وصول يُعرّض البيانات للتسريب. لذلك يُعتمد على **تشفير البيانات الساكنة** (Data at Rest)وأنظمة التحقيق الرقمي.

5. **مرحلة الإتاحة والاستخدام** :تتطلب ضوابط وصول صارمة وفق مبدأ الامتياز الأدنى وفصل المهام، بحيث لا يحصل أي مستخدم على أكثر مما يحتاج.

6. **مرحلة الحذف أو الأرشفة** :الحذف التقليدي غير كافٍ، لذا يُستخدم التدمير الكامل (Wiping) أو التشفير المسبق لضمان الإتلاف الآمن .

**أدوات الحماية المحورية**

- **التشفير** :حصن البيانات في كل المراحل (أثناء النقل، السكون، أو حتى التشغيل). يجعل البيانات بلا معنى من دون المفتاح الصحيح.
- **التحكم في الوصول** :يوزع الثقة بوعي ويراقب الصلاحيات بشكل مستمر.
- **النسخ الاحتياطية** :خطة إنقاذ لا قيمة لها بلا اختبار استعادة. تُخزن في بيئات آمنة مثل التخزين البارد وتُراجع دوريًا.
- **المراقبة والتحليل** :عين ثالثة تعتمد الذكاء الاصطناعي لرصد الأنماط والكشف المبكر عن التهديدات.
- **الثقافة البشرية** :العامل الأضعف والأخطر. كلمة مرور ضعيفة أو نقر على رابط خبيث قد يطيح بكل الحصون، لذلك تظل **الثقافة السيبرانية والوعي المستمر** أساس كل حماية.

إن أمن البيانات لا يحمي الملفات فقط، بل يحمي **القرار**، **السيادة**، **والثقة** .ومن يُهمل دورة حياة البيانات يسلم مفاتيح مستقبله إلى يد خفية لا يراها إلا بعد فوات الأوان.

## 1.4 الفرق بين أمن المعلومات والأمن السيبراني

قد يبدو للوهلة الأولى أن" أمن المعلومات "و"الأمن السيبراني "مصطلحان مترادفان، يدوران في فلك واحد، فكلاهما يسعى إلى الحماية، وكلاهما يتعامل مع المعرفة بوصفها أصلًا ينبغي صونه من العبث أو التلاعب أو التلف. غير أن النظرة المتعمقة تكشف عن علاقة أكثر تعقيدًا: علاقة احتواء لا مساواة، وتكامل لا تطابق. وهذا التمييز لا ينبع من ترف لغوي أو مصطلحي، بل من حاجة استراتيجية لرسم الحدود بين الفكرة والأداة، بين الأصل والتجلي، بين المبدأ والخط الأمامي للمواجهة.

**أمن المعلومات** (Information Security)

أمن المعلومات هو الإطار الفلسفي الأوسع، الذي ينشغل بجوهر المعلومة، لا بشكلها أو وسيلة حفظها. إنه يتعامل مع" المعرفة "بصفتها كيانًا يستحق الحماية، سواء كانت مكتوبة على ورق، منطوقة في محادثة، محفوظة في خزانة، أو مشفّرة في سحابة. ما يهمّه هو الحفاظ على ثلاثية الحماية الجوهرية: السرية (Confidentiality)، والسلامة(Integrity) ، والتوافر(Availability) ، المعروفة اختصارًا بـCIA.

في ظل هذا المفهوم، قد تشمل ممارسات أمن المعلومات إغلاق الخزائن، حماية الأرشيفات الورقية، فرض سياسة" المكاتب النظيفة"، وتقييد الوصول الفيزيائي، تمامًا كما تشمل التشفير الرقمي والجدران النارية. إنه حقل واسع، يمتد من غرف الاجتماعات إلى مراكز البيانات، ومن السياسات إلى السلوك البشري.

**الأمن السيبراني** (Cybersecurity)

أما الأمن السيبراني، فهو تخصص فرعي داخل مظلة أمن المعلومات، لكنه أكثر تحديدًا وتكثيفًا. إنه المعني بحماية الأنظمة الرقمية، من شبكات وسيرفرات وأنظمة تشغيل وبرمجيات وقواعد بيانات. إنه المقاتل الذي يقف على تخوم الإنترنت، يواجه في الزمن الحقيقي كل ما يتسلل: من البرمجيات الخبيثة (Malware)وهجمات التصيّد(Phishing) ، إلى هجمات الفدية (Ransomware) والهجمات المتقدمة المستمرة.(APT)

وإذا كان أمن المعلومات يُفكّر في السياسات والتصنيفات، فإن الأمن السيبراني يشتبك مع الهجمات، يلاحق الثغرات، ويُفعّل الاستجابات الفورية. الأول يرسم فلسفة الحماية، والثاني يُجسّدها عبر أدوات، ومنصات، ونماذج.

**التكامل بين أمن المعلومات والأمن السيبراني:**

**إطار استراتيجي وتقني للحماية الشمولية**

الفكرة لا تكتمل دون التطبيق، كما أن السلاح بلا وعي ليس إلا خطرًا آخر .فأمن المعلومات هو الفكرة، والأمن السيبراني هو السيف. الأول يخاطب الإدراك

الاستراتيجي، والثاني يخوض المواجهة التقنية. ومن لا يُتقن كليهما، كمن يعرف أن هناك حربًا، لكنه لا يحمل سيفًا، أو كمن يملك سيفًا، لكنه لا يعرف لِمَ يُقاتل.

رغم اعتماد المؤسسات على بيئات رقمية، إلا أن المعلومة لا تولد دائمًا في الإنترنت. قد تبدأ في تقرير ورقي، تُناقش في مكالمة هاتفية، تُنقل إلى بريد إلكتروني، وتُخزّن في سحابة عالمية. حماية هذا المسار لا تتم بنموذج واحد، بل تتطلب رؤية أمنية شمولية تُدرك كل نقطة تماس، وتربط بين الإدراك الإداري واليقظة التقنية.

## 1.5 تطوّر النموذج الأمني: التحول من النماذج التقليدية إلى النماذج المتقدمة في الأمن السيبراني

في بدايات العصر الرقمي، حين كانت الأنظمة مغلقة وشبكات المؤسسات محدودة النطاق، لم تكن الحاجة ماسّة إلى نماذج حماية متقدمة. آنذاك، اعتمدت النماذج الأمنية على فرضية رئيسية مفادها أن **الخطر يأتي من الخارج** .وبُنيت على هذا الأساس أدوات مثل:

- **الجدران النارية** (Firewalls) هو حاجز رقمي بين جهاز الكمبيوتر أو الشبكة الخاصة بك وبين الإنترنت أو الشبكات الأخرى. يعمل على مراقبة وتنظيم حركة البيانات التي تمر عبره، بحيث يسمح فقط للبيانات المسموح بها بالمرور ويمنع البيانات الضارة أو المهاجمة من الدخول. ببساطة، الجدار الناري مثل **حارس أمن** عند باب منزلك، يقرر من يدخل ومن لا يُسمح له بالدخول بناءً على قواعد معينة.
- **مكافحة الفيروسات** (Antivirus) هو برنامج يحمي جهازك من الفيروسات والبرامج الضارة. يقوم بفحص الملفات، ويكشف الأخطار، ثم يحذفها أو

يمنعها من الدخول إلى جهازك. ببساطة، يمكن تشبيهه بـــ جهاز مناعة رقمي يحمي جهازك من الهجمات والبرامج التي قد تسرق المعلومات أو تُتلف النظام.

- **أنظمة كشف التسلل** (IDS) هي **برامج أو أدوات** تراقب حركة الشبكة أو الجهاز، بهدف **اكتشاف أي نشاط غريب أو محاولة اختراق**. ببساطة، يمكن تشبيهها بـــ **كاميرا مراقبة رقمية** تراقب كل ما يحدث داخل الشبكة، وتنبهك إذا لاحظت شيئًا غير طبيعي أو مريبًا.

كانت هذه الأدوات تقوم على التعرف إلى "بصمة" التهديد المعروف، ومن ثم صده أو التنبيه بوجوده.

غير أن هذا النموذج التقليدي بدأ ينهار مع تطور البيئة الرقمية. فقد تغيّر شكل التهديدات: لم يعد المهاجم خارجيًا دائمًا، ولم يعد الهجوم واضحًا أو مباشرًا. بل ظهر خصم متخفي، ذكي، صبور، يعتمد على **الهندسة الاجتماعية**، و**الذكاء الاصطناعي**، و**التحليل النفسي للسلوك**، ويستطيع أحيانًا فهم النظام من داخله أكثر من مسؤولية.

**نموذج الثقة المعدومة**(Zero Trust)

استجابةً لهذه التحولات، برز نموذج **الثقة المعدومة** (Zero Trust) وهو إطار أمان إلكتروني يَفرض مبدأ "عدم الثقة المطلقة بأي كيان داخل أو خارج الشبكة"، ويَستلزم التحقق من الهوية والصلاحيات بشكل مستمر قبل منح الوصول إلى الموارد. ظهر كردّ على تزايد التهديدات الإلكترونية وتعقيد البنى التحتية الحديثة (مثل الحوسبة السحابية والعمل عن بُعد)، ويعتبر أحد أبرز النماذج الأمنية المتقدمة.

- كل طلب وصول يُعامل على أنه مشبوه.
- تُفرض آليات تحقق متعددة الطبقات.(Multi-Factor Authentication)
- تُستخدم تحليلات سلوكية ديناميكية لرصد الأنشطة.
- تُفعّل المراقبة المستمرة بدلاً من الاعتماد على التحقق المسبق.

بهذا، لم يَعُد الأمن السيبراني يعتمد على جدار يمنع الاختراق، بل على **منطق أمني جديد** قائم على الشك المستمر والتحقق الدائم.

**مبدأ الدفاع متعدد الطبقات**(Defense in Depth)

لتعزيز هذا التوجه، طُبّق مبدأ **الدفاع متعدد الطبقات**(Defense in Depth) **وهو استراتيجية أمان تشبه "التحصين الطبقي": إذا اخترق المهاجم طبقة واحدة، توجد سلسلة من الطبقات المتداخلة تمنع وصوله للهدف.**؛ تشمل هذه الطبقات: الأجهزة الفردية، التطبيقات، الشبكات، قواعد البيانات، والسحابة.

كل طبقة صُممت بحيث:

- تكشف محاولات التسلل.
- تربك المهاجم وتؤخره.
- تمنع الوصول غير المشروع.
- تستجيب تلقائيًا عند وقوع خرق.

**من الكشف إلى التنبؤ: الذكاء الاصطناعي في خدمة الأمن**

التحول الأكبر لم يكن في الأدوات فقط، بل في **الذهنية الأمنية** .فقد انتقلت الأنظمة من مرحلة **الكشف عن الهجوم** إلى مرحلة **التنبؤ به** .تقنيات الذكاء الاصطناعي والتعلم الآلي لم تَعُد تقتصر على مطابقة التهديدات المعروفة، بل أصبحت:

- تتعلم الأنماط السلوكية للمستخدمين والأنظمة.
- تكشف التغيرات الخفية التي قد تشير إلى تهديدات ناشئة.
- تُقدّر مستوى المخاطر قبل أن تتحول إلى كوارث فعلية .

إن التطور من النماذج التقليدية إلى النماذج الحديثة يعكس **تحولًا فلسفيًا** في الفكر الأمني:

- من الحراسة الخارجية إلى الرقابة الداخلية.
- من ردة الفعل إلى المبادرة الاستباقية.
- من الثقة الافتراضية إلى التشكيك الواعي.

وبات السؤال المركزي لم يعد" :هل هناك تهديد؟ "بل" :متى وأين وكيف سيقع التهديد القادم؟"

**نموذج الحماية الثلاثية(CIA)**

في قلب كل منظومة أمنية راشدة، ينبض نموذج ثلاثي يُعرف بـــCIA ، وهو ليس مجرد اختصـــار تقني، بل رؤية فلســـفية متكاملة لفهم الحماية في عصـــرٍ تتداخل فيه

المعلومة مع المصير. يقوم هذا النموذج على ثلاث ركائز لا يمكن فصل إحداها عن الأخرى: السرية(Confidentiality) ، السلامة(Integrity) ، والتوافر .(Availability) وهي ليست فقط عناصر هندسية تُستخدم في تصميم الأنظمة، بل قيم جوهرية تحكم العلاقة بين الإنسان والمعلومة، بين الثقة واتخاذ القرار، بين النظام والحياة.

فالسرية أولًا (Confidentiality) ليست مجرد إخفاء أو تشفير، بل هي عَقدٌ من الثقة بين المستخدم والنظام؛ وعدٌ بأن تظل البيانات مصونة من أعين لا ينبغي لها أن تراها. إنها احترام لخصوصية الفكرة، وصونٌ لهوية الفرد، ودرع يحول دون تسرب ما هو شخصي أو استراتيجي. لكن السرية وحدها، دون سلامة، قد تصبح غطاءً للزيف، وتحوّل المعلومة المحمية إلى خديعة مغلّفة.

من هنا تأتي السلامة(Integrity) ، باعتبارها الحارس الذي يصون جوهر المعلومة من العبث، ويحفظها من التحريف، سواء كان ذلك نتيجة إهمال أو هجوم متعمّد. فالمعلومة، مهما بدت محمية، إذا شُوهت أو زُيّفت، فإنها تفقد معناها، وتتحول إلى سُم في جسد القرار .إن سلامة البيانات هي ما يجعل من الأمن أداة لبناء الثقة، لا مجرد إجراء وقائي. وبدون سلامة، قد تُتخذ قرارات مصيرية بناءً على أوهام.

لكن حتى المعلومة الصحيحة والمحمية، لا تفي بغرضها إن لم تكن متاحة في اللحظة الحرجة. هنا تبرز أهمية التوافر(Availability) ، بوصفه الضمانة العملية لقدرة النظام على الاستجابة. فالمعرفة المخبأة خلف أنظمة مشلولة، لا تختلف كثيرًا عن الجهل .التوافر هو روح المعلومة، وحضورها عند النداء. وهو ما يجعل الأمن السيبراني لا يقتصر على التحصين، بل يشمل أيضًا الاستمرارية والمرونة.

وحين نتأمل هذا النموذج، نُدرك أنه ليس بنية تقنية، بل منطق وجودي لحياة المعلومة. فالمعلومة المتاحة إن كانت مزيّفة، قد تكون أداة تدمير. وإن كانت سرّية لكنها غير دقيقة، تتحول إلى خيانة معرفية. وإن كانت صحيحة وسرّية، لكنها غائبة وقت الحاجة، فهي خذلان وظيفي في لحظة مفصلية.

لذا فإن نموذج CIA لا يُدرَّس كتصنيف فني فحسب، بل يُمارس كإطار تفكير، وكوسيلة لبناء ثقافة أمنية واعية. إنه خريطة ذهنية (Mental Map) واستراتيجية عملية(Operational Strategy) ، تمتد من الخلية الرقمية الدقيقة، إلى قاعة اتخاذ القرار. نموذج يرشد العقول السيبرانية إلى بناء أنظمة لا تحتمي بالجدران وحدها، بل تتسلّح بالفهم(Understanding) ، والدقة(Accuracy) ، والاستباق (Proactiveness).

وفي زمن تكثر فيه التهديدات، وتضطرب فيه الحدود بين الهجوم والدفاع، يبقى هذا النموذج البوصلة السيبرانية (Cyber Compass) التي لا تنحرف، والمرجعية التي تُعيد تعريف الأمن لا كخوفٍ من المجهول، بل كحكمة واعية تُمسك بخيوط المجهول بيد من نور.

## 1.6 مستويات التهديد السيبراني في البيئة الرقمية

لم تَعُد الهجمات السيبرانية مجرد حوادث تقنية معزولة، بل تحولت إلى أدوات جيوسياسية، ووسائل ضغط اقتصادي، وآليات تنافس استخباراتي (ENISA, 2020; NIST, 2018).ومن ثمّ، أصبح من المستحيل فصل الأمن السيبراني عن البيئة الرقمية التي تشكل فضاءً معقدًا، تتشابك فيه الأجهزة، التطبيقات، والمنصات، حيث يختلط الخاص بالعام، والمستخدم بالمزوّد، والحماية بالخطر الكامن في صميم البنية ذاتها (ISO/IEC 27001, 2013).

إن فهم مستويات التهديد السيبراني لم يَعُد ترفًا نظريًا، بل ضرورة استراتيجية تحدد قدرة الأفراد والمؤسسات والدول على الصمود أمام مخاطر ذكية، متخفية، ودائمة التطور.(Ponemon Institute, 2022)

**المستوى الأول: البرمجيات الخبيثة**(Malware)

هي برامج ضارة تُصمم بهدف إلحاق الضرر بأنظمة الحاسوب أو سرقة البيانات أو التحكم في الأجهزة دون علم المستخدم. تشمل هذه الفئة عدة أنواع رئيسية مثل الفيروسات التي تلتصق بالملفات النظيفة وتنتشر عند تنفيذها، وبرمجيات الفدية التي تشفر الملفات وتطلب فدية مالية لفك التشفير، وأحصنة طروادة التي تتنكر كبرامج شرعية لخداع المستخدمين. للوقاية من هذه التهديدات،

- **آلية العمل** :فتح بوابات خلفية(Backdoors) ، مراقبة المستخدمين، تعديل الملفات، أو تعطيل الوظائف الحيوية.
- **التطور التقني** :من شيفرات بسيطة إلى برمجيات تستخدم الذكاء الاصطناعي والتشفير الذاتي والانتشار الذكي .
- **التأثير الاستراتيجي** :إضعاف السيطرة الداخلية وتفكيك البنية الرقمية تدريجيًا دون إنذارات مباشرة.

**المستوى الثاني: هجمات التصيّد الاحتيالي**(Phishing)

هي محاولات خداع إلكترونية تهدف إلى سرقة البيانات الحساسة (ككلمات المرور أو تفاصيل البطاقات الائتمانية) عبر انتحال هوية جهات موثوقة مثل البنوك أو المنصات الشهيرة. تعتمد على الاستغلال النفسي أكثر من الثغرات التقنية بحيث

تمثل صراعًا على الإدراك البشري فهي تعتمد على الهندسة الاجتماعية لاستغلال مشاعر الخوف أو الطمع أو الثقة.

- **آلية العمل** :رسائل بريد إلكتروني أو روابط وهمية تنتحل هوية جهات موثوقة (بنوك، منصات حكومية).
- **التأثير** :سرقة بيانات الاعتماد، كلمات المرور، أو فتح بوابات خلفية للأنظمة.
- **الجانب النفسي** :تُظهر هذه الهجمات أن العامل البشري هو الحلقة الأضعف، وأن الأنظمة التقنية تنهار إذا تم خداع المستخدم الذي يتحكم بها .

**المستوى الثالث: هجمات حجب الخدمة**(DoS/DDoS)

**هي هجمات إلكترونية تهدف إلى تعطيل الخدمات الرقمية أو الشبكات عن طريق إغراقها بكميات هائلة من الطلبات أو البيانات، مما يجعلها غير قادرة على الاستجابة للمستخدمين الشرعيين.**

هذه الهجمات لا تستهدف سرقة البيانات، بل تعطيل الأنظمة عبر إغراقها بوابل من الطلبات المزيفة باستخدام شبكات أجهزة مصابة (Botnets) .

- **آلية العمل** :استنزاف الموارد، إبطاء الأنظمة، منع وصول المستخدمين الشرعيين.
- **التأثير** :خسائر اقتصادية جسيمة، شلل في البنى التحتية الحيوية، تعطيل الخدمات الحكومية والمالية في لحظات حرجة.(NIST, 2018)

- **الاستراتيجية** :تستغل البنية نفسها كسلاح، إذ يُستخدم مبدأ الإتاحة ضد النظام بتحويل قوته إلى نقطة انهياره.

**المستوى الرابع: هجمات سلاسل التوريد**(Supply Chain Attacks)

هي هجمات إلكترونية معقدة تستهدف الجهات الخارجية الموردة للبرمجيات أو الخدمات أو المكونات المادية التي تعتمد عليها المنظمات، بهدف اختراق الأنظمة الرئيسية عبر استغلال الثقة الممنوحة لهذه الجهات. تُعتبر من أخطر التهديدات الحديثة لقدرتها على إصابة آلاف الضحايا عبر نقطة اختراق واحدة.

- **آلية العمل** :حقن الشيفرة الخبيثة في تحديثات برمجية، مكتبات مفتوحة المصدر، أو برامج من أطراف ثالثة.
- **التأثير** :زعزعة مفهوم الثقة المؤسسية، إذ لا تكون الثغرة في النظام نفسه، بل في المكونات التي تم دمجها فيه.
- **خطورة الاكتشاف** :غالبًا ما يصعب رصدها، لأن المكونات المدمجة تعامل كجزء أصيل من النظام .
- **البعد الفلسفي** :تكشف أن الخطر لا يأتي فقط من الخصم الخارجي، بل من داخل العلاقات التي تقوم على الثقة.

وهكذا تتغير أنماط المخاطر بتسارع يوازي تسارع الابتكار نفسه. فالبرمجيات الخبيثة تعمل كأمراض مزمنة، والتصيّد يهاجم الإدراك البشري، وحجب الخدمة يشل الأنظمة بالصخب، بينما تضرب هجمات سلاسل التوريد جوهر الثقة المؤسسية.

من هنا، لم يَعُد الأمن السيبراني مجرد جدار تقني للحماية، بل أصبح عقيدة استراتيجية وفلسفة إدارية، تنطلق من الإدراك والوعي قبل الأدوات، وتقوم على إعادة تقييم مستمرة للهياكل الأمنية. في عالم تُخاض فيه الحروب بالكود لا بالرصاص، تصبح المعرفة واليقظة أعظم أسلحة السيادة الرقمية.

## 1.7 تحوّلات في هندسة الدفاع السيبراني من الجدران الصلبة إلى الذكاء التفاعلي

لم يَعُد الفضاء السيبراني ساحة صراعات تقليدية يمكن عزلها بجدران تقنية، بل أصبح بيئة متشابكة تتلاشى فيها الحدود بين الداخل والخارج، وبين الثقة والاختراق. جوهر التحدي الأمني المعاصر لم يَعُد يكمن في قوة الأدوات فحسب، بل في الافتراضات الأمنية القديمة التي لم تواكب تحوّل البيئة الرقمية إلى نظام مفتوح ديناميكي.

في مواجهة هذا التحول، برزت الحاجة إلى فلسفة دفاعية جديدة لا تعتمد على المنع السلبي أو الحواجز الثابتة، بل على منظومات مرنة قادرة على التنبؤ بالتهديدات، والتكيف معها، وإدماج الوعي المؤسسي والثقافة الأمنية ضمن استراتيجيات الحماية. وهكذا، تطور الدفاع السيبراني من كونه حائطًا صلبًا إلى كونه نظامًا معرفيًا–تفاعليًا متعدد الأبعاد: تقني في أدواته، إدراكي في مقارباته، وفلسفي في جذوره.

**أولاً :فلسفة الثقة المعدومة** (Zero Trust)

في الأمن السيبراني، تشير فلسفة الثقة المعدومة إلى مبدأ أمني جذري يفترض أن لا شيء ولا أحد داخل الشبكة أو خارجها يستحق الثقة التلقائية. فلا يُفترض أن المستخدم الداخلي آمن، ولا أن الجهاز داخل المؤسسة موثوق، ولا أن الاتصال من

شبكة داخلية مضمون. بل إن كل طلب وصول يجب أن يُعامل كاحتمال تهديد حتى يُثبت العكس بالتحقق المستمر.

يُعد نموذج الثقة المعدومة (Zero Trust) من أبرز التحولات في هندسة الأمن السيبراني. يقوم على مبدأ جوهري" :لا ثقة دون تحقق.

- لا يُعتبر المستخدم داخليًا آمنًا لمجرد موقعه أو امتلاكه هوية مصادق عليها.
- كل طلب وصول يُعامل كمشبوه ويخضع لتوثيق متعدد العوامل (MFA) ومراقبة مستمرة.
- تُستخدم تحليلات السلوك والذكاء الاصطناعي لفحص الأنشطة لحظيًا.

يُمثل هذا النموذج نقلة من الثقة الافتراضية إلى التحقق المستمر، حيث تُبنى الثقة على المراجعة المستمرة للهوية والسياق، لا على الافتراضات المسبقة. فلسفيًا، يعيد Zero Trust صياغة مفهوم الثقة ذاته في الفضاء الرقمي، ويحوّله من فضيلة اجتماعية إلى معادلة أمنية دقيقة.

**ثانيًا: الدفاع متعدد الطبقات** (Defense in Depth)

هو منهج أمني استراتيجي يقوم على مبدأ أن لا توجد وسيلة حماية واحدة كافية وحدها، بل يجب بناء منظومة من الطبقات الأمنية المتتابعة والمتكاملة بحيث تُعزز كل طبقة الأخرى، وتشكل معًا جدارًا مركّبًا يصعب اختراقه، بحيث تُشكل كل طبقة عائقًا إضافيًا أمام المهاجم.

- الطبقات تشمل: المستخدم النهائي، الشبكات، التطبيقات، قواعد البيانات، والبنى السحابية.

- الهدف ليس فقط منع الاختراق، بل إبطاؤه واكتشافه وتقليل آثاره.
- يُشبه في فلسفته التحصينات العسكرية التقليدية: لا يُحمى القصر بسور واحد، بل بخنادق وأسوار متتابعة وأبراج مراقبة.

هذا النموذج يعكس واقعية استراتيجية: يفترض أن الاختراق قد يحدث، لكن يراهن على أن الطبقات المتعددة ستمنح المؤسسة وقتًا حاسمًا للتصدي والاحتواء. وهو ما يُجسّد قيمة المرونة والاستمرارية في مواجهة الهجمات.

**ثالثًا :الأمن التكيّفي** (Adaptive Security)

ظهر نموذج الأمن التكيّفي (Adaptive Security) استجابة لبيئة تهديد ديناميكية، يتغير فيها الخطر بسرعة تفوق التوقعات. وهو نموذج أمني ديناميكي يعتمد على المراقبة المستمرة، والتحليل اللحظي، والتعلم الآلي للتكيف تلقائيًا مع طبيعة التهديدات المتغيرة، بحيث يتطور النظام الأمني باستمرار بدلًا من أن يبقى ثابتًا أمام هجمات متجددة.

بمعنى آخر، هو **أمن يتعلم ويتطور مع الزمن**. فبدل أن يستجيب للهجوم بعد وقوعه، يسعى **للتنبؤ به والتكيّف معه قبل حدوثه** من خلال الذكاء الاصطناعي والتحليل السلوكي.

التوقعات. يقوم هذا النموذج على أربعة أعمدة:

1. **الرصد المستمر** لسلوك الأنظمة والمستخدمين.
2. **التحليل** باستخدام الذكاء الاصطناعي لاكتشاف الأنماط والشذوذ.

3. **الاستجابة التلقائية** عبر عزل الجلسات أو تقييد الصلاحيات.

4. **التكيف** من خلال إعادة برمجة الدفاعات بناءً على الخبرة المكتسبة من الهجمات2021 (Gartner, 2021).؛ FireEye, 2021).

يمثل الأمن التكيّفي انتقالًا من ردة الفعل إلى الفعل الاستباقي، ومن الجمود إلى التعلم المستمر .إنه نظام يتطور مع كل هجوم، يحوّل كل حادثة إلى درس، ويجعل البنية الأمنية أكثر نضجًا مع مرور الوقت.

### التكامل بين النماذج

رغم اختلاف الأسس، إلا أن النماذج الثلاثة تتكامل في إطار واحد:

- Zero Trust يطرح سؤال :من أنت؟
- Defense in Depth يطرح سؤال :ماذا لو؟
- Adaptive Security يطرح سؤال :ماذا بعد؟

هذه الأسئلة لا تعكس الخوف بقدر ما تعكس الوعي السيبراني الناضج، الذي يدرك أن التهديد لم يعد يأتي من الخارج فقط، بل من الداخل، وأن الأمن لا يُبنى على الافتراضات، بل على التحقق والمرونة والاستبصار.

إن هندسة الدفاع السيبراني لم تَعُد تقوم على الجدران الصلبة وحدها، بل على عقل أمني تفاعلي يدرك أن الخطر جزء من البيئة الرقمية ذاتها. فالثقة المسبقة أصبحت ثغرة، والجمود ضعفًا، بينما الذكاء التفاعلي والقدرة على التعلم المستمر يمثلان جوهر الحماية المعاصرة. ومن هنا، لا تُقاس قوة المنظومة بعدد أدواتها فقط، بل بقدرتها على التكيف، والاستمرارية، وبناء الثقة المكتسبة لا المفترضة.

## 1.8 الاتجاهات الحديثة في الأمن السيبراني

لم تعد التهديدات السيبرانية تنشأ من فجوات في أنظمة مغلقة أو أجهزة معزولة، بل باتت تتكاثر في فضاءات مترابطة، تتسع مع انتشار الحوسبة السحابية، وتتغلغل في الأنظمة الصناعية، وتنتشر في كل جهاز متصل بالشبكة .(ENISA, 2020) ومع هذا التحول، لم تعد النماذج الأمنية التقليدية قادرة على مواكبة خطورة البيئات الجديدة، مما أدى إلى بروز اتجاهات متقدمة تعيد صياغة ماهية الحماية، وتقدم حلولًا تخصصية ومرنة ذات بعد استباقي عميق.

**أولًا: أمن الحوسبة السحابية – تحوّل في المفهوم قبل التقنية**

الحوسبة السحابية (Cloud Computing) هي نموذج لتقديم خدمات الحوسبة — مثل الخوادم، والتخزين، وقواعد البيانات، والشبكات، والبرمجيات — عبر الإنترنت ("السحابة")، بدلاً من الاعتماد على البنية التحتية المحلية. أي أن المستخدم يمكنه الوصول إلى الموارد الحاسوبية وتشغيلها عند الطلب (On-Demand)من أي مكان، دون الحاجة إلى امتلاكها أو إدارتها فعليًا.

أحدثت الحوسبة السحابية تحولًا بنيويًا عميقًا في البنية التحتية الرقمية، إذ انتقلت المؤسسات من امتلاك مواردها التقنية إلى استئجارها عبر مزودي خدمات سحابية. هذا التحول منح المؤسسات **مرونة تشغيلية**، و**توفيرًا في الموارد**، و**قدرة عالية على التوسع**، لكنه رافقه تحديات أمنية استراتيجية.

**من أبرز هذه التحديات:**

- **فقدان السيطرة المباشرة على البيانات** في بيئات مشتركة متعددة العملاء، مما يزيد احتمالية التسريب.

- **ثغرات الواجهات البرمجية** (APIs) التي تُستغل في الهجمات نتيجة سوء التكوين أو غياب الضبط.
- **توزيع المسؤوليات الأمنية** بين مزود الخدمة والمستخدم النهائي، مما قد يخلق ثغرات تشغيلية عند غياب الوضوح .

للتقليل من هذه المخاطر، تُجمِع الأدبيات المتخصصة على حزمةٍ متكاملة من الضوابط تجمع بين التحصين التقني والحوكمة التشغيلية :

بدءًا بالتشفير من طرف إلى طرف للبيانات أثناء النقل والتخزين لضمان السريّة وسلامة المحتوى، مرورًا بإدارة الهويات والصلاحيات (IAM) وفق مبدأ الامتياز الأدنى لتقليص مساحة الهجوم، وتفعيل منصّات المراقبة والتحليل (SIEM)لربط الأحداث واكتشاف الشذوذ مبكرًا، وصولًا إلى سياسات وصول ديناميكية تعتمد على الهوية والسياق (هوية المستخدم، الجهاز، الموقع، درجة المخاطرة اللحظية) بما يضبط القرار النفاذي لحظيًا بدل الاكتفاء بضوابط ساكنة (Gartner, 2021).وعلى المستوى المعماري، تؤكد المقاربات الحديثة ضرورة الانتقال من حماية «المحيط» إلى مبدأ التحقق المستمر وافتراض الاختراق كما في نموذج انعدام الثقة(Zero Trust) ، حيث يصبح الأمن قائمًا على التثبت المتكرر وتحليل السلوك وليس على مجرد وجود الأصل داخل الشبكة . بهذه الرؤية، لا تُعد الحوسبة السحابية مجرّد بيئة تشغيل جديدة، بل إعادة صياغة لمفهوم الأمان نفسه: من الاعتماد على الموقع إلى حماية كل معاملة وكل هوية، على مدار اللحظة

.

**ثانيًا: أمن إنترنت الأشياء – تأمين الذكاء المتناثر في تفاصيل الحياة**

إنترنت الأشياء (IoT) هو شبكة من الأجهزة والأشياء المادية المتصلة بالإنترنت ، مثل الحساسات، الكاميرات، السيارات، الأجهزة المنزلية، والأنظمة الصناعية — والتي تستطيع جمع البيانات وتبادلها وتحليلها دون تدخل بشري مباشر، بهدف اتخاذ قرارات ذكية وتحسين الأداء والراحة والكفاءة. بمعنى آخر، هو تحويل العالم المادي إلى منظومة رقمية متصلة وواعية بالبيئة المحيطة بها. ورغم بساطة وظائفها، فإن هذه الأجهزة تشكل نقاط دخول عالية الخطورة إذا لم تُؤمَّن.

**التحديات الرئيسة:**

- القدرات الحاسوبية المحدودة للأجهزة، مما يصعّب تحميلها بحلول حماية تقليدية.
- افتقار العديد من الأجهزة إلى تصميم أمني مدمج، إذ صُمّمت لأداء مهام تشغيلية قبل مراعاة البعد الأمني.
- إمكانية تحوّل اختراق جهاز بسيط (مثل كاميرا) إلى نقطة وصول لشبكات مركزية حساسة .

**الحلول المقترحة:**

- تبنّي مبدأ **الأمن المدمج في التصميم**.(Security by Design)
- **تحديثات دورية للبرمجيات الثابتة** (Firmware Updates) لسد الثغرات.
- بروتوكولات **تشفير خفيفة وآمنة** تناسب محدودية الأجهزة.

- دمج الأجهزة في أنظمة مركزية لإدارة الهوية والصلاحيات (ISO/IEC 27001, 2013).

يمثل أمن إنترنت الأشياء جزءًا من فلسفة الأمن الموزع، حيث تنتشر المخاطر عبر "الأشياء الصغيرة"، وتتطلب حلولًا **خفيفة ومرنة واستباقية.**

**ثالثًا: أمن الأنظمة الصناعية – حماية القلب التشغيلي للبنية التحتية**

هي مجموعة من الأنظمة التقنية والهندسية التي تُستخدم لإدارة وتشغيل العمليات الصناعية والإنتاجية في المصانع والمنشآت الحيوية، مثل أنظمة التحكم بالمحطات الكهربائية، ومصافي النفط، وخطوط التصنيع، ومنشآت المياه والنقل. ورغم أنها صُممت للعمل في بيئات معزولة، فإن التحول الرقمي وربطها بالشبكات العامة جعلها أهدافًا مباشرة للهجمات.

تشمل هذه الأنظمة عادةً ما يُعرف بـــ أنظمة التحكم الصناعي (Industrial Control Systems – ICS)، مثل:

- أنظمة التحكم الإشرافي وجمع البيانات(SCADA)
- أنظمة التحكم المنطقي المبرمج(PLC)
- وأنظمة التحكم الموزعة(DCS)

وتهدف إلى ضمان التشغيل المستمر، الدقيق، والآمن للعمليات الصناعية عبر مراقبة المعدات، تحليل البيانات، وضبط العمليات في الوقت الحقيقي.

في المفهوم السيبراني، تُعد الأنظمة الصناعية من الأصول الحرجة (Critical Infrastructure)التي تتطلب حماية خاصة، لأنها تمثل نقطة التقاء بين العالمين

الفيزيائي والرقمي، وأي اختراق فيها قد يؤدي إلى أضـــرار مادية جســـيمة أو توقف خـدمـات وطنيـة. لـذا يُطبَّق عليهـا الأمن الســـيبراني الصـــنـاعـي Industrial) (Cybersecurityالذي يجمع بين معايير السلامة التشغيلية والأمن المعلوماتي.

**مكامن الخطورة:**

- قدم هذه الأنظمة وعدم مراعاتها لمتطلبات الأمن الحديثة.
- صعوبة تحديثها بسبب طبيعة العمليات الحرجة.
- غياب معايير موحدة لحمايتها عبر مختلف المصنعين.

**آليات الحماية:**

- الفصل الدقيق بين بيئات تقنية المعلومات (IT) وتقنيات التشغيل.(OT)
- بناء أنظمـة مراقبـة قـادرة على رصـــد أي نشـــاط غير اعتيـادي دون تعطيـل العمليات.
- إعداد خطط استجابة مرنة لا تتطلب إيقاف المنشآت الحيوية.
- تطبيق مفهوم **الدفاع في العمق** مع التركيز على العنصـــر البشـــري والتدريب الأمني.

أمن الأنظمـة الصـــنـاعيـة ليس خيارًا تكميليًا، بل أحد أعمدة الســـيادة الرقمية للدولة، وأساسًا لضمان أمن الطاقة والمياه والغذاء والنقل والإنتاج.

توضـــح الاتجاهات الحديثة في الأمن الســـيبراني أن التحديات لم تعد مقتصـــرة على حماية الأنظمة المغلقة، بل أصـــبحت تمتد إلى البيئات الســـحابية، شـــبكات

إنترنت الأشـياء، والأنظمة الصـناعية. هذه البيئات تتطلب حلولًا متخصـصـة، مرنة، واستباقية، تقوم على الثقة المحدودة، الرقابة المستمرة، والتكامل بين التقنية والثقافة الأمنية .ومن دون هذا الفهم الاسـتراتيجي، قد تتحول البنى الرقمية من ركيزة للتنمية إلى نقطة ضعف تهدد الأمن الوطني ذاته.

## خاتمة الفصل

بعد استعراض النماذج الدفاعية المتقدمةZero Trust — ، Defense in Depth، و — Adaptive Securityيمكن القول إن الأمن السيبراني الحديث لم يَعُد مجرد تقنيات وأدوات، بل أصبح إطارًا استراتيجيًا متكاملًا يجمع بين الفكر، والسياسة، والتقنية، والثقافة المؤسسية.

لقد عبّر "سن تزو" في كتابه *فن الحرب* عن جوهر الفلسفة الأمنية حين قال:

"إذا عرَفت نفسك وعرَفت عدوّك، فلن تخشى مائة معركة؛ وإن عرَفت نفسك ولم تعرف عدوّك، فلك انتصار وهزيمة؛ وإن لم تعرف نفسك ولا عدوّك، فالهلاك حتمي. *(Sun Tzu, trans. 2005)* "

وهذا المعنى يتجسد في نموذجZero Trust ، الذي يقوم على إعادة تعريف الثقة. فمعرفة الذات تُترجم إلى إدارة دقيقة للهويات والصلاحيات، ومعرفة العدو تتحقق عبر التحليل السلوكي والمراقبة المستمرة. إن غياب أي منهما يجعل احتمالية الفشل ليست مجرد احتمال، بل نتيجة مؤكدة.

وكما كتب سن تزو" :*الهجوم هو سر الدفاع؛ والدفاع هو خطة للهجوم.*"

وهو ما يعكس جوهر Defense in Depth، إذ لا يكفي الاعتماد على طبقة واحدة أو جدار حماية صلب لمواجهة خصوم يستخدمون الذكاء الاصطناعي والهندسة الاجتماعية. الدفاع الفعّال اليوم هو دفاع ديناميكي، متعدد الطبقات، قادر على الردع والاكتشاف والرد الاستباقي، بحيث يتحول من موقع الدفاع إلى الهجوم عند الضرورة.

ويضيف سن تزو" :*القادر على التكيّف والتغيّر حسب العدو ويحقق النصر، يُقال عنه الإله.*"

وهذا القول يختصر فلسفة Adaptive Security، حيث لم يَعُد الثبات مجديًا في عالم تتبدل فيه التهديدات لحظيًا. إن القدرة على الرصد، والتحليل، والاستجابة اللحظية، والتكيف المستمر مع بيئة متغيرة، هي ما يضمن بقاء المنظومات الرقمية آمنة وقادرة على الصمود.

إن ما نستخلصه من هذه النماذج أن الأمن السيبراني الحديث تجاوز مرحلة كونه مجموعة من الأدوات الدفاعية، ليصبح عقيدة سيادية واعية .فهو لم يَعُد يقتصر على جدران حماية أو برامج مضادة للفيروسات، بل تحول إلى هندسة متقدمة ترى في كل ثغرة فرصة للفهم، وفي كل تهديد مجالًا للتطور، وفي كل تفاعل اختبارًا للثقة (Schneier, 2015).

وفي عالم تُقاس فيه قيمة البيانات بما يفوق قيمة النفط، وتتشابك فيه بيئات السحابة، وإنترنت الأشياء، والأنظمة الصناعية، تصبح هذه النماذج الدفاعية فلسفات عملية للوجود الرقمي .(ENISA, 2020; Ponemon Institute, 2022) إنها تحدد ليس فقط كيف نمنع الهجمات، بل كيف نفكر ونُقيّم ونُدير الثقة في فضاء تتآكل فيه الحدود، وتصبح الثقة فيه موردًا نادرًا وأصلًا استراتيجيًا.

الأمن السيبراني، في ضوء هذه النماذج، لم يَعُد حالة دفاعية فحسب، بل ممارسة سيادية قائمة على المعرفة، والتحليل، والمرونة. إنه دفاع يستمد قوته من الحكمة القديمة، لكنه يتجسد اليوم في دروع رقمية حديثة قادرة على حماية الأفراد، والمؤسسات، والدول في زمن السيولة الرقمية.

إن الخلاصة الكبرى لهذا الفصل، أن الأمن السيبراني يبدأ من العقلية، ويترسخ بالثقافة، ويستدام بالمرونة والتعلّم .ومن دون هذا الفهم الاستراتيجي، قد تتحول البنى الرقمية من رافعة للتنمية إلى نقطة ضعف تهدد الهوية والسيادة. أما المؤسسات والدول التي تُدرك هذه الحقيقة، فهي الأقدر على بناء فضاء رقمي آمن وسيادي، قادر على مواجهة المستقبل بثقة وحكمة.

# الفصل الثانيِ

## (مدخل الى السيادةَ الرقَميةَ)

# مقدمة الفصل

لقد تحوّل الفضـاء الرقمي إلى "وطنٍ موازٍ" لا تُقاس حدوده بالكيلومترات، بل بالحزم الرقمية، ولا تحرسه الجيوش، بل أنظمة التشفير، ومراكز البيانات، وشبكات الاتصالات العابرة للقارات.

**السيادة الرقمية**، وفق هذا المنظور، هي قدرة الدولة على اتخاذ قراراتها الرقمية باستقلال كامل، بعيدًا عن التبعية لمزودات أجنبية أو برمجيات لا تخضع لسلطتها التشريعية. إنها تعني امتلاك البنى التحتية الرقمية، والتحكم في تدفق البيانات، وصياغة التشريعات السيبرانية الوطنية التي تضمن حماية الهوية والاستقلالية

لقد تغيّر وجه الأمن القومي؛ فلم يعد يرتكز على حماية الخنادق أو الأسلحة التقليدية، بل على حماية الخوادم، مفاتيح التشفير، والبنية التحتية السيبرانية. اليوم تُقاس قوة الدولة بقدرتها على الصمود أمام الهجمات الإلكترونية وحماية بيانات مواطنيها من التسريب والاستغلال.

بدأ ظهور مفهوم **التحول الرقمي** بأنه استخدام التكنولوجيا الرقمية لتحسين وتطوير الأعمال والعمليات في المؤسسات. وكان يعرّف ببساطة، على انه عملية تحويل الأنشطة التقليدية التي كانت تتم يدويًا إلى أنشطة تعتمد على التكنولوجيا مثل الإنترنت، البرمجيات، والأجهزة الذكية. بهدف جعل العمل أكثر كفاءة وسرعة، وتحسين تجربة العملاء، وتوفير حلول مبتكرة للتحديات اليومية.

ولكنه يبرز اليوم بُعدًا فلسفيًا عميقًا. إذ أنّ الاعتماد المفرط على الوسائط الرقمية يعيد تشكيل البنية الإدراكية للإنسان، منتجًا عقلًا سريعًا، متشظيًا، أقل قدرة على التركيز العميق. هذا التحول المعرفي لا يقتصر على الأفراد، بل يمتد ليعيد

صياغة علاقة الدولة بمواطنيها، حيث لم تعد السلطة تُمارس فقط عبر الرقابة التقليدية، بل عبر إدارة تدفقات المعلومات وتنظيم فضاء الوعي الجمعي.

إن من يملك البنية التحتية الرقمية يملك القدرة على تشكيل السلوك والتحكم في المعنى ذاته. وبالتالي، فإن السيادة الرقمية لا تنحصر في البنى التقنية، بل تمتد إلى السيادة المعرفية، أي حق الدولة في حماية وعيها الجمعي من الاستلاب عبر منصات أجنبية وخوارزميات تجارية لا تراعي الخصوصية الثقافية والسياسية المحلية.

بذلك، يتضح أن التحول الرقمي ليس مجرد مشروع تقني لتحديث المؤسسات، بل هو مشروع سيادي وفكري يعيد تعريف الدولة، والمواطنة، والهوية في زمن تُقاس فيه القوة بمدى التحكم في البيانات والخوارزميات، لا بعدد الجنود أو حجم السلاح. فمن لا يملك مفاتيح بنيته الرقمية، يخاطر بفقدان استقلاله، وربما وجوده ككيان سيادي.

يركّز هذا الفصل على الفرق بين أمن المعلومات والسيادة الرقمية، مبينًا أن الحماية التقنية لا تكفي دون امتلاك القرار الوطني على البيانات والبنية التحتية. يناقش مفهوم الحوكمة الرقمية كأداة للسيادة، ويعرض أطرًا عملية لفهم العلاقة بين الأمن والقرار.

## 2.1 السيادة الرقمية وأمن المعلومات: من حماية البيانات إلى امتلاك القرار

في قلب الدولة الحديثة ينهض سؤال لم يعد ممكنًا تجاهله: هل نملك بياناتنا فعلًا، أم أننا نكتفي بحمايتها؟ قد يبدو السؤال تقنيًا في ظاهره، لكنه في حقيقته سؤال سيادي وجودي. فالتشفير والجدران النارية، مهما بلغت قوتها، لا تعني بالضرورة أننا نمتلك القرار. تمامًا كما أن وضع حارس على باب البيت لا يعني أنّ الملكية

عائدة لصــاحبه. هنا يظهر الفارق الجوهري بين **أمن المعلومات** و**الســيادة الرقمية** : الأول ينشــغل بالدفاع عن القلعة، بينما الثاني يحدد من يبنيها، ومن يضــع قوانينها، ومن يملك مفاتيحها.

لقد نشــأ مفهوم أمن المعلومات من منطلق الخوف: الخوف من الاختراق، من التلاعب، من الفقدان أو الســرقة. فجاءت الاســتجابة عبر ثالوث الحماية المعروف: الســرية(Confidentiality) ، الســلامة(Integrity) ، والتوافر(Availability) الذي تحدثنا عنه في الفصــل الأول. هذا الثالوث أفرز آلاف الأدوات الأمنية؛ من الجدران النارية، إلى أنظمة التشــفير، إلى التوثيق متعدد العوامل. لكنها جميعًا ظلت تدور حول ســؤال واحد :*كيف نحمي ما بين أيدينا؟* غير أنها لم تجب على ســؤال أعمق : *هل ما نحميه ملكٌ لنا أصلًا؟*

من هنا ظهر مفهوم الســيادة الرقمية، ليخرج من دائرة التقنية الضــيقة إلى فضــاء القرار الوطني. المسألة لم تعد مجرد حماية أنظمة أو تشفير بيانات، بل امتلاك القرار في لحظة الأزمة: هل تُخزَّن بيانات الدولة على أرضها أم في خوادم أجنبية؟ هل تصوغ الدولة خوارزمياتها بنفســها أم تعتمد على برمجيات مغلقة المصــدر صُــممت في بيئة قانونية لا تخضــع لها؟ وهل تستطيع في لحظة الخطر أن توقف تدفق بياناتها السيادية دون إذن خارجي؟

المفارقة أن دولًا كثيرة تطبّق أعلى معايير أمن المعلومات، ومع ذلك تعيش في تبعية رقمية ناعمة. فبياناتها محفوظة في مراكز أجنبية، وبناها التحتية الســحابية مُدارة عبر منصات لا تملك شيفرتها المصدرية، وقوانينها السيبرانية خاضعة لمعايير تُصاغ

خارج حدودها. تبدو محمية تقنيًا، لكنها فاقدة للمفتاح السـيادي. فالقفل بلا مفتاح ليس أمنًا، بل وهم أمني يخفي هشاشة داخلية.

وتتعاظم الإشكالية أكثر مع صعود الخوارزميات والمنصات الرقمية. فهي لم تعد أدوات محايدة، بل قوانين خفية تعيد تشكيل الواقع. محركات البحث تُبرز نتائج وتُخفي أخرى، ومنصات التواصل تصوغ الرأي العام عبر خوارزميات التوصية التي تحدد ما نراه وما نتجاهله. وهكذا، باتت الخوارزميات تمارس سـلطة فوق سـيادية، تُعيد هندسة الوعي الجمعي دون شفافية أو مساءلة.

وتجاوز الأمر حدود الخوارزميات إلى الشركات التقنية العملاقة (مثل Google و Metaو Amazonو Microsoft) التي تحوّلت إلى كيانات سـيادية بلا أعلام. فهي من تضع القوانين عبر "شروط الخدمة"، وهي من تسمح وتحجب دون الرجوع إلى برلمانات، وهي من تتحكم في تدفقات البيانات والسلوك الجمعي على نطاق يتجاوز قدرة حكومات كثيرة.

الدولة التي لا تمتلك بدائل محلية ولا أدوات رقمية خاصـة سـتظل رهينة لهذه القوى، حتى وإن رفعت شعار "الأمن السيبراني."

لهذا، فإن السـيادة الرقمية ليسـت مجرد خيار تقني، بل مشـروع وجودي. إنها امتلاك الخوادم والبنى التحتيـة، والسـيطرة على البروتوكولات، وصـيـاغـة الخوارزميات المحلية، وتحديد السـياق المعرفي الذي تُبنى فيه الحقيقة. إنها حماية للإدراك الجمعي من أن يُعاد تشكيله وفق قيم لا تعبّر عن المجتمع المحلي.

في المحصـلة، يمكن القول إن **أمن المعلومات يمنح الطمأنينة، لكن السـيادة الرقمية تمنح الحرية** .فالحماية تُبقي الجدران قائمة، بينما السـيادة تمنحنا الحق في وضـع قوانين البيت وتحديد من يملكه. وفي عالم تجاوزت فيه الخوارزميات حدود الأدوات لتصبح أدوات سلطة، لم يعد الأمن وحده كافيًا. الشرط الحقيقي للوجود السيادي هو أن نمتلك القرار الرقمي من الجذر إلى القمة.

## 2.2 الحوكمة والحوكمة الرقمية: من ضبط القرار المؤسسي إلى إعادة تشكيل السيادة الرقمية

**الـــحوكمة** ليست مجرد مصطلح إداري متداول، بل منظومة متكاملة تنظم العلاقة بين مختلف الأطراف داخل أي مؤسسة: من صناع القرار والإدارة التنفيذية، إلى الجهات الرقابية وأصـحاب المصـلحة. وهي لا تُختزل في الهيكل الإداري أو اللوائح الرسمية، بل تمتد إلى رسم السياسات، وتوزيع المسؤوليات، وضبط آليات المساءلة والتقييم المستمر.

بهذا المعنى، تعدت الحوكمة مفهومها التقليدي بأنها مجموعة من المبادئ والقواعد التي تهدف إلى تنظيم إدارة المؤسـسـات أو الدول بطريقة شـفافة، عادلة، وفعّالة، وأنها عملية اتخاذ القرارات وتوزيع السلطة داخل الكيانات المختلفة لضمان تحقيق الأهداف بشـكل منظم ومسـؤول. بل باتت تمثل الإطار الذي يوازن بين الأهداف الاستراتيجية للمؤسسة من جهة، والالتزامات الأخلاقية والاجتماعية من جهة أخرى.

لقد نشـأ هذا المفهوم في الأصـل كرد فعل على الأزمات المؤسـسـية وأوجه القصور التي شهدتها بيئات العمل خلال العقود الماضية، ثم تطور ليصبح اليوم أحد

أعمدة الإدارة الحديثة. فالمؤسسة التي لا تعتمد حوكمة واضحة تشبه سفينة بلا بوصلة؛ قد تملك المحرك والطاقم، لكنها تفتقد الاتجاه والثقة. أما حين تتبنى فلسفة الحوكمة، فإنها تُعزز الشفافية، وتبني الثقة مع بيئتها الداخلية والخارجية، وتضمن أن قراراتها لا تُتخذ بمعزل عن القيم والنزاهة والاستدامة.

هي فلسفة عمل تُرسخ المسؤولية وتحوّلها إلى ثقافة مؤسسية. إنها العقد غير المكتوب بين المؤسسة ومجتمعها، الذي يضمن أن السعي وراء الكفاءة والربح لن يكون على حساب الأخلاق أو المصلحة العامة.

### 2.2.1 من الحوكمة التقليدية إلى الحوكمة الرقمية

مع التحولات العميقة التي جاء بها التحول الرقمي، لم تَعُد المؤسسات تعمل في فضاء مادي بحت، بل أصبحت تُدار عبر بيئات رقمية متعددة الأبعاد. هذا الواقع الجديد لم يُغيّر أدوات العمل فحسب، بل غيّر فلسفة الإدارة نفسها، ودفع بمفهوم الحوكمة إلى التوسع والتكيف، ليولد منه مفهوم الحوكمة الرقمية.

فالتحول هنا ليس مجرد انتقال من الورق إلى الشاشة، أو من المكتب إلى المنصة، بل هو انتقال فلسفي ومعرفي شامل. لم تَعُد السلطة تُمارَس من خلال هياكل جامدة وقرارات بيروقراطية بطيئة، بل باتت تُعاد صياغة العلاقة بين السلطة والمعرفة، وبين الإنسان والآلة، وبين المواطن والدولة، داخل فضاءات رقمية ديناميكية وسريعة الإيقاع.

الحوكمة الرقمية إذن ليست امتدادًا تقنيًا للحوكمة التقليدية، بل مشروع جديد لإعادة تعريف السلطة نفسها في عصر السيادة الرقمية. هي الإطار الذي يجعل البيانات موردًا سياديًا، والذكاء الاصطناعي شريكًا في القرار، والمنصات الذكية

أدواتٍ لتفعيل الشفافية والرقابة. إنها ببساطة إعادة كتابة قواعد اللعبة المؤسسية، لكن بلغة الخوارزميات هذه المرة.

**طبيعة الحوكمة الرقمية**

الـحوكمة الرقمية هي الإطار الذي يوجّه كيفيّة استخدام التكنولوجيا الحديثة في إدارة المؤسسات والدول والمجتمعات. إنها لا تعني مجرد إدخال الحاسوب أو الإنترنت في العمل الإداري، بل تمثّل تحولًا جذريًا في طريقة اتخاذ القرار وتنظيم العلاقة بين المواطن والدولة في فضاء متصل ومفتوح على الدوام.

وتقوم الحوكمة الرقمية على مجموعة من الأبعاد المتشابكة التي لا يمكن فصل أحدها عن الآخر:

- **السياسات الرقمية** :وضع قواعد واضحة لإدارة البيانات والخدمات، بما يضمن وضوح المسار ومرونة التكيف مع التغيرات.
- **الأمن السيبراني** :حماية البنى التحتية الرقمية من التهديدات، وضمان استمرارية الخدمات بلا انقطاع.
- **الخصوصية وحقوق المستخدم** :تشريعات تضع حدودًا فاصلة بين ما يحق للدولة أو المؤسسة جمعه من بيانات، وبين ما يجب أن يبقى ملكًا للفرد وحريته.
- **الشفافية الرقمية** :الانتقال من تقارير ورقية بطيئة إلى بيانات مفتوحة يمكن الوصول إليها وتحليلها لحظيًا، ما يعزز الثقة والمساءلة.

وعبر هذه الأبعاد، تصبح الحوكمة الرقمية أداةً لتجسيد قدرة الدولة أو المؤسسة على التحكم والإشراف وتوجيه المسارات الرقمية بما يخدم المصلحة العامة. فهي الإطار الذي يضمن أن التكنولوجيا ليست مجرد أداة، بل وسيلة لتحقيق العدالة، تكافؤ الفرص، وضمان الحقوق في عالم لم يعُد يعترف بالفواصل التقليدية بين الواقعي والافتراضي.

### 2.2.2 مقارنة بين الحوكمة التقليدية والرقمية

بينما كانت الحوكمة التقليدية تقوم على أدوات مألوفة مثل الاجتماعات، المحاضر الورقية، والتقارير الدورية، جاءت الحوكمة الرقمية لتستبدل ذلك كله بأنظمة مؤتمتة وسلاسل بيانات وخوارزميات تحليلية تعمل في الزمن الحقيقي. فالرقابة لم تَعُد مؤجلة إلى نهاية الشهر أو السنة، بل أصبحت مراقبة آنية مستمرة. والشفافية لم تَعُد محصورة في تقرير رسمي يصدر دوريًا، بل تحوّلت إلى بيانات مفتوحة يمكن تحليلها ومراجعتها لحظيًا.

وإذا كان الهدف في الحوكمة التقليدية هو بناء الثقة المؤسسية بين الموظف والإدارة وبين المؤسسة ومحيطها، فإن الحوكمة الرقمية تسعى إلى ما هو أبعد: بناء **الثقة الرقمية** .هذه الثقة لا تتحقق إلا عندما يشعر المواطن أو المستخدم أن بياناته مؤمّنة، وأن القرارات التي تُبنى على الخوارزميات شفافة وعادلة، وأن العدالة الرقمية لا تقل شأنًا عن العدالة الإدارية.

بهذا المعنى، فإن التحول من الحوكمة التقليدية إلى الحوكمة الرقمية هو انتقال من **نزاهة إدارية** تُقاس بسلوك الأفراد والإجراءات، إلى **نزاهة رقمية** تُقاس بسلامة

البيانات، موثوقية الأنظمة، وعدالة القرارات التي تصدر عنها. إنها نقلة نوعية لا تقتصر على تغيير الأدوات، بل تعيد صياغة مفهوم الثقة ذاته في زمن السيادة الرقمية.

**البعد السيادي للحوكمة الرقمية**

لا يمكن الحديث عن الحوكمة الرقمية بمعزل عن بعدها السيادي. ففي عالم تُمارَس فيه السلطة عبر المنصات والخوارزميات، لم تعُد الحوكمة الرقمية مجرد أداة لإدارة العمليات التقنية، بل غدت شرطًا أساسيًا لحماية استقلال القرار الوطني. إنها الإطار الذي يحدد إن كان القرار الرقمي يُصاغ داخل حدود الدولة أم يُفرض عليها من الخارج، وإن كانت البيانات والخدمات تُدار وفق تشريعات محلية أم تخضع لقوانين غريبة عنها.

بهذا المعنى، تصبح الحوكمة الرقمية ركيزة للسيادة الرقمية؛ فهي لا تكتفي بتنظيم العلاقة بين المواطن والدولة في الفضاء الرقمي، بل تُعيد تعريف هذه العلاقة وفق قيم الاستقلال والحرية والعدالة. ومن خلالها يتحدد موقع الدولة في النظام الرقمي العالمي: هل هي فاعل مستقل يصوغ قواعده، أم تابع يتلقى ما يُفرض عليه من معايير؟

## 2.3 الحوكمة الرقمية والسيادة الرقمية: جدلية الأداة والغاية

برز مفهومان متلازمان في المظهر، مختلفان في الجوهر :الحوكمة الرقمية والسيادة الرقمية .الفارق بينهما ليس تفصيلًا شكليًا، بل جوهريًا؛ أشبه بالفارق بين من يملك أدوات الإدارة ومن يملك حق الإدارة ذاته.

**الحوكمة الرقمية: إطار الإدارة والتنظيم**

التحول الرقمي ليس مجرد استخدام للتطبيقات أو الحواسيب، بل إعادة تشكيل لطريقة اتخاذ القرار. هنا تبرز الحوكمة الرقمية كإطار تنظيمي وتقني يمكّن الحكومات من إدارة شؤونها عبر منصات ذكية وسلاسل بيانات مترابطة. هدفها تحسين الأداء المؤسسي، رفع كفاءة الخدمات، تعزيز المشاركة المجتمعية، وضمان المساءلة في الزمن الحقيقي.

من التصويت الإلكتروني إلى المرور الذكي، ومن العدالة الرقمية إلى الشفافية في الموارد، تجسد الحوكمة الرقمية نقلة من البيروقراطية الثقيلة إلى إدارة أكثر تفاعلية ومرونة. لكنها تظل مشغولة بالسؤال :كيف ندير؟ أكثر مما تهتم بالسؤال :لمن ندير؟

**السيادة الرقمية: امتلاك القرار والتحكم**

أما السيادة الرقمية فتنظر إلى ما وراء الكفاءة. إنها تعنى بالسؤال الجوهري: من يملك البنية التحتية الرقمية؟ من يكتب الخوارزميات الوطنية؟ من يتحكم في تدفق البيانات ويملك مفاتيح التشفير؟

الدولة التي تدير خدماتها بكفاءة عالية لكنها تخزّن بياناتها في خوادم أجنبية أو تعتمد على برمجيات مغلقة المصدر لا تخضع لقوانينها، تمارس حوكمة بلا سيادة. إنها تُشبه فنانًا يزيّن جدارًا في بيت مستأجر: قد يكون العمل متقنًا، لكن قرار الطرد يظل بيد المالك.

**بين الحوكمة والسيادة: معادلة القوة الرقمية**

الخلل يتجلى في حالتين متناقضتين:

- **حوكمة بلا سيادة** :إدارة كفؤة لكنها مرتهنة لبنى وأدوات خارجية.
- **سيادة بلا حوكمة** :امتلاك للبنية والموارد الرقمية، لكن بلا قدرة على إدارتها بكفاءة.

القوة الحقيقية تولد من التكامل بين الاثنين: حوكمة رشيدة داخل نظام سيادي مستقل.

**الشركات العملاقة ككيانات ما فوق–سيادية**

يزداد المشهد تعقيدًا مع بروز شركات التكنولوجيا الكبرى كـ"دول بلا أعلام". فهي من تضع قوانينها عبر شروط الاستخدام، وتتحكم في تدفقات البيانات، وتمارس سلطة فعلية على المجتمعات تتجاوز سلطة كثير من الحكومات.

**المبادرات الدولية: محاولة لإعادة التوازن**

في مواجهة هذا الواقع، ظهرت مبادرات مثل GAIA-X الأوروبي الذي يسعى لبناء سيادة سحابية أوروبية، و"إعلان جنيف الرقمي" الذي يؤكد على الحقوق الرقمية، إلى جانب تحالفات إقليمية مثل Cyber Shield أو المبادرات العربية للأمن السيبراني. لكنها لا تزال تصطدم بعقبات تفاوت القدرات وضعف التشريعات الموحدة.

**إشكالية التوازن: انفتاح أم انغلاق؟**

التحدي الأكبر اليوم هو صياغة معادلة بين الانفتاح السيبراني وحرية تدفق المعلومات من جهة، وحماية السيادة الوطنية من الاختراق والهيمنة من جهة أخرى. فالعزلة الرقمية غير ممكنة، والانفتاح المطلق غير آمن. المطلوب هو نموذج متوازن قائم على العدالة الرقمية، الخصوصية كحق سيادي، والشفافية في الخوارزميات والبنى التنظيمية.

**الحوكمة أداة، والسيادة غاية**

في فلسفة الدولة الرقمية الحديثة:

- **الحوكمة الرقمية** هي الأداة التي تنظّم الأداء وتُحسّن الكفاءة.
- **السيادة الرقمية** هي الغاية التي تمنح الشرعية والاستقلال.

فلا جدوى من حوكمة بلا سيادة تحميها، ولا معنى لسيادة بلا حوكمة تُترجمها إلى واقع. وبين هذين البعدين، تُرسم اليوم معالم الدولة الرقمية: إنسانية في جوهرها، سيادية في قرارها، ومستدامة في تطورها.

## 2. أزمة القرار السيبراني: من امتلاك البنية إلى امتلاك الإرادة

الخطر في الفضاء السيبراني لا يأتي دائمًا من هجوم مباشر أو فيروس مدمر، بل من خوارزمية غامضة تُعيد ترتيب الأولويات دون أن ننتبه، أو سياسة خصوصية تغيّر قواعد اللعبة في الخلفية. التهديد الأخطر اليوم ليس فقط اختراق الشبكات، بل القدرة على إعادة تشكيل الوعي الجمعي والتحكم في تدفق المعرفة، بحيث تُوجَّه الدول والمجتمعات في مسارات صُممت خارج حدودها.

### 1. الانكشاف الخفي: الاعتماد على بنى غير مملوكة

الانكشاف الحقيقي لا يتمثل في هجوم واضح، بل في الاعتماد على منصات وبنى تحتية لا نملكها. دول كثيرة، حتى الكبرى منها، تبني خدماتها على أنظمة تشغيل مغلقة المصدر أو على خوارزميات ذكاء اصطناعي تديرها شركات عابرة للقارات. في هذه الحالة تصبح حماية البيانات مشروطة بقرارات كيانات خاصة، قادرة على تعطيل الخدمة أو التحكم بها في أي لحظة توتر سياسي.

### 2. البنية وحدها لا تكفي

امتلاك مراكز بيانات وطنية أو شبكات محلية مشفرة لا يعني بالضرورة امتلاك القرار. السؤال الأعمق: من يُدير هذه الأنظمة؟ ومن يملك حق تعديلها أو تعطيلها عند الأزمات؟ السيادة لا تُقاس بالمعدات وحدها، بل بقدرة العقول الوطنية على فهم البنية والتحكم بمسارها.

### 3. معضلة الكفاءات والاعتماد على الخارج

كثير من الدول تستعين بخبرات أجنبية لإدارة بنيتها الرقمية. لكنها بذلك تستورد التقنية ومعها احتمالات النفوذ السياسي. النتيجة: منظومات متطورة ظاهريًا، لكنها تُدار بعقول مستعارة، فتتحول الرقمنة من أداة للتمكين إلى أداة للتبعية.

### 4. التشريع والسياسة: شرط الكرامة الرقمية

حتى أقوى البنى الرقمية لا تعني شيئًا إذا لم تسندها قوانين وطنية صارمة، وتشريعات تفرض السيادة على البيانات، وتضع الخصوصية في صميم القرار. من دون إطار قانوني واضح، يتحول "الاستقلال الرقمي" إلى شعار سياسي بلا مضمون.

وهكذا، تتضح ملامح مشروع جديد يمكن تسميته بـــ الكرامة الرقمية .ليس بمعناها الرمزي، بل بمعناها العملي: امتلاك الخوارزميات محليًا، تخزين البيانات داخل الحدود، الإشراف المباشر على البنية الرقمية، وإنتاج المعرفة بدل استيرادها. فالسيادة لا تُشترى بالأجهزة، بل تُبنى بالإرادة والعقول.

**السيادة المشفّرة: كيف يُعاد تشكيل الوعي بالخوارزميات**

أدوات القوة الجديدة لا تفجر المدن، بل تُعيد تشكيل العقول. الخطر لم يَعُد في احتلال الأراضي، بل في السيطرة على تدفقات البيانات التي تصنع وعي الأفراد والمجتمعات.

**1. الشركات ككيانات فوق–سيادية**

شركات مثل Google و Metaو Amazonو Microsoftلم تعد مجرد شركات تجارية، بل تمارس نفوذًا يفوق سلطة دول بأكملها. تحديث صغير في سياسة الخصوصية أو خوارزمية ترتيب النتائج كفيل بإعادة صياغة أولويات مجتمع بأسره.

**2. الخوارزمية كأداة هيمنة ناعمة**

محركات البحث لا تنقل المعلومات بحياد، بل تعيد ترتيبها وفق منطق مبرمج مسبقًا. منصات التواصل لا تكتفي بربط الناس، بل تعيد تشكيل المجال العام نفسه، تُخفي خطابًا وتضخّم آخر، لتصنع واقعًا بديلًا يبدو طبيعيًا بينما هو مصمَّم بعناية.

**3. السيادة الإدراكية: اختراق المعنى لا البنية**

الاختراق الأخطر يتم داخل الإدراك: من يحدد قيم الجمال والنجاح؟ من يكتب وعي الأطفال والمراهقين؟ من يصوغ "الترند" الذي يُعيد تشكيل الثقافة؟ الدولة التي لا تكتب خوارزمياتها ولا تنتج محتواها، تسلّم تشكيل أجيالها إلى قوى خارجية.

### 4. مأزق الدولة بين الانفتاح والانصياع

الحكومات عالقة بين خيارين: إما التكيّف مع منطق المنصات الكبرى بما يحمله من فقدان للسيادة الناعمة، أو الانعزال الرقمي بما يحمله من اتهام بالانغلاق. وكلاهما وصفة للتبعية ما لم يُصَغ بديل وطني متوازن.

### 5. من السيادة التقنية إلى السيادة المعرفية

حتى لو امتلكت الدولة أنظمتها، فإن غياب السيطرة على الخوارزميات يجعلها مجرد مستخدم داخل بيئة لم تصممها. السيادة الحقيقية اليوم هي امتلاك حق تشكيل الإدراك، لا مجرد حماية البنية.

### نحو مشروع سيادة رقمية حقيقية: ثلاثية القرار السيادي

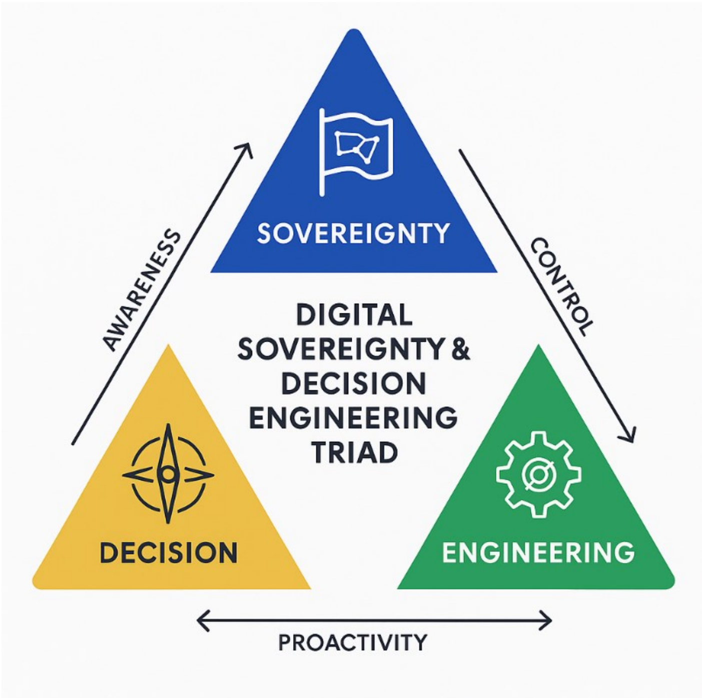
قوة الدولة الحديثة تُقاس اليوم بثلاثية مترابطة:

1. إرادة سياسية واعية :تشريعات وطنية تضع السيادة الرقمية فوق مصالح الشركات الكبرى.
2. استقلال تقني استراتيجي :بنى وطنية، خوارزميات محلية، تقليل الاعتماد على البرمجيات المغلقة.
3. ثقافة رقمية مجتمعية راشدة :مواطنون يفهمون كيف تُعيد الخوارزميات تشكيل وعيهم، ويمارسون النقد الواعي للمنصات.

هذه الثلاثية ليست خطة تقنية، بل مشروع حضاري يحوّل الدولة من متلقٍ للتقنية إلى صانع لمستقبله. فالسيادة اليوم لا تُقاس بالحدود الجغرافية، بل بامتلاك

مفاتيح الفضـــاء الرقمي. من يكتب الخوارزمية يكتب الوعي، ومن يكتب الوعي يكتب المستقبل.

### 2.4 نموذج مثلث السيادة الرقمية




**الشكل( 2.1) نموذج السيادة الرقمية**

يطمح مثلث الســيادة الرقمية وهندســة القرار كما في النموذج إلى أن يكون إطارًا اسـتراتيجيًا عالميًا، يقود الدول والمؤسـسـات نحو امتلاك قرارها السـيبراني في مواجهة عالم يزداد تعقيدًا وتشـابكًا. فالرؤية التي يحملها هذا النموذج تتجاوز حدود الحماية التقنية إلى صـياغة قوة جديدة، حيث تصـبح البيانات والخوارزميات أدوات سيادة، والهندسة السيبرانية فنًّا لتصميم البنى التحتية المحصّنة، والقرار لحظة الحسم التي تترجم الوعي والسيطرة إلى فعلٍ سيادي متكامل.

تقوم فلسفة هذا النموذج على قناعة جوهرية بأن الأمن السيبراني لم يعد مجرد درع يحمي من المخاطر، بل أصبح شرطًا وجوديًا يحدد قدرة الدولة أو المؤسسة على الاستمرار والازدهار. فالسيادة هنا ليست شعارًا بل ممارسة عملية في امتلاك مفاتيح البيئة الرقمية، والهندسة ليست إجراءً تقنيًا بل رؤية لبناء منظومات مقاومة وصامدة، أما القرار فهو تجسيد للحظة الحقيقة؛ حيث يلتقي العلم بالزمن، وتتحول الضغوط والتهديدات إلى فرص لإعادة تشكيل المصير.

ومن هذه الرؤية والفلسفة تنبثق رسالة النموذج: تمكين الدول والمؤسسات من بناء سيادة رقمية حصينة تحمي هويتها وإرادتها، وتطوير هندسة قرار سيبراني ترتكز على الذكاء الاصطناعي والتحليل الاستباقي، وصولًا إلى قرارات سريعة وفاعلة تحوّل التهديدات إلى مسارات قوة. إنها رسالة تؤكد أن الأمن السيبراني ليس مجرد دفاع عن حدود افتراضية، بل هو بناء سيادة معرفية وقرار سيادي في قلب العاصفة الرقمية.

## خاتمة الفصل

لقد تحوّل مفهوم الأمن في العصر الرقمي ليصبح القدرة على رسم المسارات المعلوماتية وتوجيهها، لا الاكتفاء ببناء جدران حماية. ومع هذا التحوّل، لم تَعُد السيادة الرقمية ترفًا فكريًا أو خيارًا سياسيًا، بل صارت شرطًا وجوديًا لبقاء الدولة واستقلالها. فالدولة التي تستورد أدواتها الرقمية دون أن تملك التحكم في شيفراتها، إنما تُسلّم قرارها – طوعًا أو غفلة – إلى قوى خارج حدودها. وكل خوارزمية تُستخدم بلا وعي نقدي أو سيطرة سيادية تحمل خطر إعادة تشكيل الإدراك الجمعي من خارج الوطن.

ما تكشفه هذه الرؤية أن الحماية لم تَعُد في الجدران النارية وحدها، بل في امتلاك المفاتيح التي تتحكم فيها: متى تُفتح ومتى تُغلق، وكيف تُوجّه أو يُعاد تشكيلها. الدولة التي تعتمد على تحديث خارجي أو تخزن بياناتها في مراكز سحابية أجنبية قد تبدو محمية، لكنها مفرغة من مضمون القرار السيادي.

الأدبيات الحديثة تؤكد هذه الحقيقة: شوشانا زوبوف تحذر من تحويل البيانات إلى أداة هيمنة، وماريانا ماتزوكاتو تدعو إلى أن تتحول الدولة من مستهلك للتكنولوجيا إلى مُنتِج سيادي للبنية الرقمية. يفغيني موروزوف يكشف وهم حرية الإنترنت المفتوحة، ونيكولاس كار ينبه إلى خطورة الاستهلاك الرقمي غير الناقد على بنية العقل الجمعي. أما يوفال نوح هراري فيرى أن معارك المستقبل ستُحسم عبر القدرة على التنبؤ بسلوك الإنسان بالبيانات، في حين يحذر كلاوس شواب من أن من يتخلف عن الرقمنة يُقصى تلقائيًا من مائدة القرار العالمي.

هذه الرؤى جميعها تتقاطع في خلاصة واحدة :من لا يملك كوده، لا يملك قراره. ومن لا يملك قراره، لا يملك مستقبله .فالدولة التي لا تصوغ معمارها الرقمي لا تملك سيادتها. والاستراتيجيات الوطنية والتقارير الدولية – مثل الاستراتيجية السعودية للتحول الرقمي، وتقييم ENISA لتوجهات التهديدات، وإطار NIST للأمن السيبراني – تؤكد جميعها أن حماية البنية الرقمية لم تَعُد رفاهية تقنية، بل ضرورة وجودية.

لكن الإدراك وحده لا يكفي، إذ يجب أن يتحوّل إلى مشروع وطني متكامل يقوم على ثلاث ركائز مترابطة:

1. إرادة سياسية واعية تُجرؤ على مقاومة التبعية الرقمية.
2. استقلال تقني استراتيجي يضمن السيطرة على البنى والخوارزميات.
3. ثقافة رقمية مجتمعية راشدة تحمي الوعي من الاستلاب الخفي.

فكما كانت الدول في الماضي تبني حصونها من الحجارة، فهي اليوم مطالبة ببناء حصونها من الشيفرات. وكما كانت السيادة تُقاس بقدرة الجيوش على حراسة الحدود، فهي اليوم تُقاس بقدرة الدول على حماية قرارها في الفضاء الرقمي.

وفي النهاية، يمكن تلخيص الدرس المركزي لهذا الفصل في معادلة واحدة: من لا يملك الكود، لا يملك القرار. ومن لا يملك قراره، لا يملك مستقبله. فالسيادة لم تَعُد تُكتب على الخرائط، بل تُكتب الآن في سطور البرمجة التي تحدد: حرية أم استلاب، استقلال أم تبعية، حضور أم غياب في المشهد العالمي.

# الفصل الثالث

# هندسة القرار السيبراني

# المفهوم والأدوات

# مقدمة الفصل

هنا، حيث يشتبك الزمن بالمعرفة، يصبح سؤال البقاء مرهونًا بالقدرة على الإجابة عن أسئلة مصيرية: من يرصد أولًا؟ من يحلّل أسرع؟ من يقرّر أدق؟ ومن يمتلك شجاعة التصرف وسط ضباب المعلومات؟ لم تعُد هذه الاستفسارات شأنًا تقنيًا صرفًا، بل تحولت إلى معضلات وجودية تمس الأمن الوطني والسيادة الرقمية معًا.

في هذا السياق، بزغت هندسة القرار السيبراني بوصفها إطارًا معرفيًا متقدّمًا يعيد تعريف عملية اتخاذ القرار في العصر الرقمي. فالقرار لم يعد مجرد اختيار بين بدائل جاهزة، بل أصبح منظومة هجينة يتداخل فيها العقل البشري مع قدرات الخوارزميات، ويتكامل فيها التحليل الإدراكي مع المعالجة الآلية للبيانات. إننا أمام صياغة جديدة للقرار، لا بوصفه مهارة إدارية محدودة، بل كركيزة سيادية ترسم حدود الفعل في عالم تحكمه السرعة، الغموض، والتعقيد البنيوي.

فالقرار في بيئة المعلومات المتدفقة لا ينتظر اكتمال المعطيات، لأنه لو فعل يكون قد تأخر. المعلومة إذا وصلت متأخرة تصبح بلا جدوى، والخوارزمية إذا تلكأت في إصدار توصيتها قد تُفقد المؤسسة أو الدولة قدرتها على المواجهة. ومن هنا، تتجاوز هندسة القرار السؤال البديهي "ماذا نقرّر؟" لتطرح أسئلة أعمق وأكثر خطورة: متى نتخذ القرار؟ كيف نصمم البنية الذهنية والتقنية التي تنتج القرار الصحيح؟ وما المعايير التي ينبغي إخضاعها للاختبار تحت ضغط الزمن والخطر؟

إنها منظومة تقوم على تداخل معارف متشابكة. فهي تستمد من نظرية القرار أدواتها لتحليل البدائل تحت ظروف عدم اليقين، وتستعين بـ نظرية الألعاب لفهم الخصم والتنبؤ بسلوكه، وتستند إلى تحليل المخاطر لتقدير كلفة الاحتمالات وتأثيراتها الاستراتيجية، وتعتمد على تقنيات الذكاء الاصطناعي لتحويل الضجيج الرقمي إلى أنماط ومعرفة قابلة للتنفيذ عبر أنظمة دعم القرار الذكي والتعلّم الآلي وتحليلات البيانات الضخمة.

وتتجسد هذه الرؤية في نماذج عملية أثبتت جدواها، مثل نموذج OODA Loopالذي يختصر دورة القرار في أربع مراحل: المراقبة، توجيه الإدراك، اتخاذ القرار، والتنفيذ. أو نموذج Cyber Kill Chain الذي يفكك مراحل الهجوم الإلكتروني إلى حلقات متتابعة تمنح المدافعين فرصًا متعددة للتدخل المبكر. هذه النماذج ليست نظريات جامدة، بل أدوات يومية تُستخدم في غرف العمليات السيبرانية حيث تُقاس القرارات بالثواني، ويصبح الخطأ مكلفًا، والتردد قاتلًا.

وبذلك، تتضح مكانة هندسة القرار السيبراني كفنّ للنجاة وعلم للبقاء في عالم لا يرحم المترددين. فهي توازن بين الخطأ المكلف والصواب غير المكتمل، بين الجرأة والحذر، وتحوّل لحظة الأزمة إلى اختبار لمدى نضج الرؤية المؤسسية وقدرتها على تحويل الغموض إلى مسار استراتيجي مدروس. ومن هنا، يمكن القول إن هندسة القرار ليست خيارًا إضافيًا، بل ضرورة وجودية لكل كيان رقمي يسعى إلى حماية ذاته وصياغة مستقبله. فمن لا يُحسن هندسة قراراته، سيجد نفسه في النهاية تابعًا لقرارات صاغها غيره، وربما مرهونًا بخوارزميات لم يُشارك في كتابتها.

### 3.1 تعريف هندسة القرار في السياق السيبراني

في الفضاء السيبراني المعاصر، حيث تتكاثر البيانات بمعدلات فلكية تتجاوز قدرة البشر على الاستيعاب، وحيث تتشابك التهديدات داخل منظومات عابرة للحدود تتسم بالغموض والسرعة، لم تعد صناعة القرار مجرّد إجراء إداري أو عملية تنظيمية محدودة. لقد تحولت إلى هندسة معرفية خوارزمية معقّدة، تتداخل فيها الخوارزميات مع الإدراك البشري، وتتفاعل فيها المعطيات الرقمية مع الرؤية الاستراتيجية، لتُنتج قرارًا لا يقوم على الحدس وحده، بل على فهم معمّق لمعادلات المخاطر والإمكان.

هذه الهندسة لا تُعنى بالقرار كاختيار لحظي بين بدائل كما صوّرها هربرت سايمون في نظرياته الكلاسيكية، بل تتعامل معه بوصفه منظومة كاملة تمتد عبر الزمن. إنها المنهجية التي تُحوّل الضجيج المعلوماتي إلى رؤية واضحة، وتحوّل حالة الطوارئ إلى خريطة احتمالات، وتعيد ترتيب الأولويات في بيئة لا تمنح ترف التجريب، ولا تسمح بتكرار الأخطاء. ومن هنا، أصبحت هندسة القرار السيبراني علمًا قائمًا بذاته، يتقاطع مع نظرية القرار، علم البيانات، الذكاء الاصطناعي، والسياسات السيبرانية.

وما يميز السياق السيبراني أن القرار فيه لا يُبنى على الوقائع المكتملة، بل على استشراف المستقبل. فالمعلومة التي تصل متأخرة تصبح بلا قيمة، والخوارزمية التي تتردد في تقديم توصية قد تكلف المؤسسة وجودها. ولذلك، يقوم القرار السيبراني على الاستباق: استشراف السيناريوهات، توقع سلوك العدو قبل ظهوره، وتحويل الأنماط الخفية إلى إشارات قابلة للتحليل والتوظيف .هنا يتجلى جوهر ما أشار إليه

مالكولم غلادويل في كتابه Blink بأن الذكاء الحقيقي لا يُقاس فقط بصحة القرار، بل بسرعة اتخاذه قبل فوات الأوان.(Gladwell, 2005)

هذا التحول يجعل من القرار السيبراني فنًا للتوازن بين الصواب غير المكتمل والخطأ المكلف، بين الجرأة والحذر، وبين الإقدام والتريّث. فالبيئة الرقمية محكومة بثلاث خصائص قاتلة: الغموض المعرفي الناتج عن نقص أو تضليل في المعلومات، السرعة القسرية التي تفرض اتخاذ القرار في ثوانٍ، والتعقيد البنيوي الذي يدمج الأبعاد التقنية بالسياسية والقانونية معًا. في ظل هذه السمات، يصبح القرار السيبراني أكثر من مجرد فعل إداري، بل عملية وجودية تختبر كيان الدولة والمؤسسة معًا.

وعلى هذا الأساس، تُعرّف هندسة القرار السيبراني بوصفها جبهة استراتيجية متقدمة، تستند إلى دمج ثلاثة أبعاد مترابطة: التحليل الكمي عبر النمذجة الاحتمالية وتحليل المخاطر، الذكاء الاصطناعي القادر على التعلّم من أنماط الهجمات وتقديم توصيات تنبؤية في الزمن الحقيقي، والإدراك البشري الذي يمنح القرار بعده السيادي والأخلاقي. هذا التكامل بين الإنسان والآلة، أو ما يُعرف بالشراكة البشرية الخوارزمية وهو ما يجعل القرار السيبراني ممكنًا وفعالًا في آن.

لكن هندسة القرار ليست مجرد استجابة للحظة الأزمة، بل هي منظومة مستمرة تُدمج في البنية الرقمية منذ البداية. فهي تسأل: كيف نُصمم البنية التحتية لتكون مرنة أمام التهديدات؟ كيف نُدرّب الموظف لاتخاذ القرار الصحيح في أقل من دقيقة؟ كيف نُعد الأنظمة للتنبؤ بالاحتمالات قبل أن تتحول إلى هجمات؟

وكيف ندمج القرار داخل المعمار الرقمي ذاته، لا كإجراء إضـافي، بل كوظيفة حيوية للبقاء.

بهذا المعنى، يصـبح القرار السـيبراني كيانًا حيًا يتنفس داخل البنية الرقمية، يتطور مع الزمن، ويسـتجيب للأزمات دون أن يفقد جذوره في العمق الاسـتراتيجي. إنه ليس فعلًا فرديًا معزولًا، بل منظومة متشـابكة يُعاد اختبارها وتطويرها باسـتمرار عبر المحاكاة، السيناريوهات التفاعلية، ومراكز التدريب السيبراني.

هكذا، يتضـح أن القرارات الأمنية لم تعد قرارات طارئة، بل تحولت إلى نمط بنيوي من الفعل المنظّم والمتكيّف .إنها ممارسـة سـيادية جوهرية في عالم يتسـع فيه الخطر بقدر ما يتسـع فيه الطموح. فمن لا يُحسـن هندسـة قراراته، سـيجد نفسـه محكومًا بخوارزميات لم يكتبها، ويخضع لمعادلات لم يُشارك في صياغتها. ولهذا، تمثل هندسة القرار السيبراني اليوم ليس فقط ركيزة للأمن، بل أساسًا للسيادة ذاتها في عصر تُكتب فيه القوة بلغة الكود لا بلغة السلاح.

## 3.2 علوم اتخاذ القرار تحت التهديد في البيئة السيبرانية

يشـهد الفضـاء السـيبراني اليوم تحوّلًا جذريًا في طبيعة اتخاذ القرار؛ فلم يعد الأمر متعلقًا بانتقاء البدائل في أوقات الاسـتقرار، بل بات تحديًا وجوديًا يتجلّى في لحظات الضغط، حيث تهيمن السرعة، الغموض، والاحتمال على كل حركة. إنّ هذا التحول يعكس مقولة الفيلسوف اليوناني أرشيلوكوس" :*في أوقات التهديد، لا نرتقي إلى مستوى توقعاتنا، بل ننخفض إلى مستوى تدريبنا*"، وهي قاعدة فلسفية وعملية تُستخدم اليوم في العلوم العسكرية والإدارية لتأكيد أن القرارات الرشـيدة لا تُبنى في لحظة الأزمة، بل تُصـاغ عبر التدريب المسـبق، والمحاكاة، والنماذج التفاعلية (Kahneman, 2011).

في البيئات الرقمية عالية الخطورة، يصبح القرار فعلًا فوريًا يتطلّب دقة استثنائية واستجابة ضمن هامش زمني بالغ الضيق. وهنا تظهر الحاجة إلى تكامل مجموعة من العلوم التي تشكّل الأساس المنهجي لهندسة القرار السيبراني: نظرية القرار، نظرية الألعاب، والنمذجة الاحتمالية. هذه الحقول لا تعمل منفصلة، بل تتداخل ضمن منظومة سيادية تُحوّل الضباب المعلوماتي إلى مسارات واضحة، وتمنح المؤسسة قدرة على تحويل الخطر إلى احتمالات مُسيطر عليها.

### 3.3.1 نظرية القرار (Decision Theory) موازنة البدائل تحت عدم اليقين

تمثل نظرية القرار حجر الأساس في التعامل مع البيئات المعقدة حيث تغيب المعلومات الكاملة ويتقدم الغموض على اليقين. فهي لا تهدف إلى إنتاج القرار "المثالي"، بل القرار "الأمثل الممكن" الذي يوازن بين احتمالية النجاح وكُلفة الفشل ضمن ظروف ضاغطة.

في السياق السيبراني، تتحوّل هذه النظرية إلى بوصلة داخل الضباب، تُساعد صانع القرار على تحديد الاتجاه الأكثر توازنًا حين تكون المعلومات ناقصة، والتهديدات متعددة، والزمن ضاغط. وتُوظّف عبر أدوات مثل مصفوفات القرار وتحليل المنفعة المتوقعة (Expected Utility Analysis)، لتقدير البدائل ليس فقط وفق جدواها التقنية، بل وفق أثرها الاستراتيجي على السيادة الرقمية واستمرارية الأعمال.

إنّ تطبيقات هذه النظرية تتجسد عند مواجهة قرارات مصيرية: هل يتم إيقاف النظام المصاب؟ هل يُعلن الهجوم إعلاميًا أم يُعالج بصمت؟ كيف تُدار الأولويات

حين تتقاطع اعتبارات تقنية مع تداعيات سياسية وقانونية؟ هنا لا يصبح القرار مجرد خيار لحظي، بل أداة سيادية تعكس وعي المؤسسة بمصيرها في لحظة الخطر.

### 3.3.2 نظرية الألعاب (Game Theory) فهم سلوك المهاجمين وتوقّع خطواتهم

تُضيف نظرية الألعاب بعدًا استراتيجيًا إلى هندسة القرار، فهي تُحاكي سلوك الخصم وتفترض كيف سيُعيد صياغة استراتيجياته استنادًا إلى قراراتك. في الأمن السيبراني، حيث يختفي الفاعلون خلف هويات مزيفة وهجمات متكررة، تتحول هذه النظرية إلى أداة تحليلية لفهم ديناميكيات "اللعبة" بين المدافع والمهاجم.

على سبيل المثال، في سيناريو هجوم الفدية(Ransomware) ، قد يختار المهاجم التشفير والابتزاز، بينما يوازن المدافع بين الدفع أو الاعتماد على النسخ الاحتياطية. إدراك المهاجم لسياسة المؤسسة (مثل "لا تفاوض") يغير من حساباته في الهجوم التالي. كذلك تُستخدم استراتيجيات مختلطة (Mixed Strategies) للحفاظ على حالة من عدم اليقين لدى المهاجم، مما يرفع تكلفة التنبؤ بسلوك المدافع.

الألعاب المتكررة والألعاب ذات المعلومات غير الكاملة تُبرز أيضًا قيمة الخداع السيبراني (Cyber Deception)كاستراتيجية ردعية، عبر أدوات مثل أنظمة "الهونيپوت" التي تُربك المهاجم وتكسر يقينه. وهكذا، لا تعود القرارات السيبرانية ردود فعل معزولة، بل تصبح جزءًا من لعبة استراتيجية معقّدة تُبنى على الحساب والتوقّع، لا على العشوائية.

### 3.3.3.النمذجة الاحتمالية (Probabilistic Modeling) الاستباق عبر خرائط المستقبل

إذا كانت نظرية القرار تحدد البدائل، ونظرية الألعاب تفكك سلوك الخصم، فإن النمذجة الاحتمالية تمنح صانع القرار "ذاكرة مستقبلية" تُقدّر الخسائر المحتملة وتبني سيناريوهات استباقية للتعامل مع أخطر الاحتمالات.

وفي البيئة السيبرانية، لا تكفي الحسابات المالية أو التقنية وحدها لتقدير حجم الخطر، إذ تمتد آثار الهجوم إلى أبعاد أعمق تشمل فقدان ثقة المواطنين، والانهيار المعنوي للمؤسسة، والتبعات القانونية أو الدبلوماسية المحتملة.

هنا تبرز أهمية النماذج التحليلية المتقدمة مثل تحليل المخاطر البايزي (Bayesian Risk Analysis)، وهو أسلوب يتعلّم من التجربة، يبدأ بتقدير مبدئي للمخاطر ثم يُحدّث هذا التقدير باستمرار بناءً على المعطيات الجديدة ليقدّم توقعًا أدق لاحتمال الخطر وتأثيره.

وكذلك محاكاة مونت كارلو(Monte Carlo Simulation) ، التي تعتمد على التكرار العشوائي للتجارب لاختبار مئات أو آلاف السيناريوهات المختلفة، من أجل استشراف النتائج الممكنة عندما تكون الظروف غير مؤكدة.

بهذه الأدوات، يتحوّل الغموض إلى احتمالات قابلة للقياس، ويصبح اتخاذ القرار السيبراني أكثر وعيًا واستباقية، قائمًا على تحليل علمي يقلّل المفاجآت ويُعزّز القدرة على الصمود.

النمذجة الاحتمالية لا تُزيل الخطر، لكنها تنزع عنه عنصـر المفاجأة. فهي لا تجيب فقط :ما احتمال وقوع الهجوم؟، بل :ما الثمن المتوقع إذا وقع؟ وما أفضـل لحظة للتدخل لتقليل أثره؟، وهكذا تتحول القرارات من ردود فعل متأخرة إلى أفعال استباقية مبرمجة ضمن نطاق الاحتمالات.

### 3.3.4 نحو تكامل العلوم في لحظة التهديد

إنّ هندسة القرار تحت التهديد ليست ممارسة منعزلة، بل مسرح تتكامل فيه العلوم: نظرية القرار توفر العقلانية، نظرية الألعاب تقدم الاستراتيجية، والنمذجة الاحتمالية تمنح الاستباق. جميعها تلتقي لتُنتج قرارًا سياديًا قادرًا على الصمود وسط الغموض والضغط والسرعة.

فالقرار السيبراني ليس مجرد اختيار بديل، بل فعل سيادي يُعيد تعريف الوعي في زمن تُصاغ فيه المعارك بالكود والخوارزميات أكثر مما تُصاغ بالحدود والجيوش. ومن لم يُحسن هندسة قراراته تحت الضغط، قد يجد نفسه في النهاية محكومًا بقرارات صاغها خصومه قبله.

### 3.4.أدوات الذكاء الاصطناعي الداعمة لصناعة القرار الأمني

كما ذكرنا سابقا،ان القرار في البيئة الرقمية لم يعد مسألة جودة تقنية فقط، بل مسألة توقيت أيضًا؛ إذ قد يكون القرار صحيحًا من حيث المضمون، لكنه يفقد قيمته إذا تأخر عن لحظة الحسم. وهنا يتجلى البعد المعرفي العميق الذي أشار إليه دانيال كانيمان (Kahneman, 2011) حين أكد أن سرعة اتخاذ القرار في ظل عدم اليقين لا تقل أهمية عن دقته. وفي السياق نفسه، يرى ديرك هيلبنغ (Helbing, 2019) أن العالم

الرقمي بات يفرض على المؤسسات أن تبني قراراتها ضمن بيئة ديناميكية متغيرة، حيث يصبح التنبؤ والقدرة على الاستبصار شرطًا للسيادة، لا مجرد ميزة إضافية.

إن هذه التحولات تكشف أن التحدي الحقيقي لم يعد في امتلاك أدوات الحماية وحدها، بل في هندسة القرار ذاته: كيف يُصاغ؟ متى يُتخذ؟ وكيف يُدمج في منظومة سيادية قادرة على الاستجابة قبل أن تتفاقم التهديدات؟

إنّ الاعتماد على الذكاء البشري وحده، مهما بلغت فطنته، أصبح غير كافٍ؛ فالعقل البشري مبدع في القيادة والتقدير، لكنه لا يستطيع بمفرده مراقبة ملايين الإشارات الشبكية، وتحليلها، وربطها في الزمن الحقيقي. وهنا يظهر الذكاء الاصطناعي (AI) لا كبديل عن الإنسان، بل كشريك استراتيجي يوسّع مداه، ويُحرره من عبء التفاصيل، ويتيح له التركيز على ما يُميز دوره: القيادة، والتقدير، واتخاذ القرارات السيادية.

في هذا السياق، يمكن تصنيف أدوات الذكاء الاصطناعي الداعمة لصناعة القرار الأمني ضمن أربع ركائز أساسية، تعمل بشكل متكامل يشبه دماغًا سيبرانيًا مؤسسيًا واعيًا.

1. **أنظمة دعم القرار الذكي**(Intelligent Decision Support Systems - IDSS)

تُعدّ **أنظمة دعم القرار الذكي** الطبقة التنفيذية التي تربط البيانات بالقرار. فهي لم تعد مجرد أدوات عرض رسومية أو لوحات مؤشرات، بل أصبحت أنظمة تحليلية متكاملة، قادرة على دمج البيانات التشغيلية في الزمن الحقيقي مع قواعد معرفية متراكمة لتوليد توصيات قابلة للتنفيذ.

في الأمن السيبراني، تعمل هذه الأنظمة كوسيط بين الفوضى والمعالجة، إذ تقوم بإعادة تنظيم الإشارات المتناثرة (مثل محاولات تسجيل الدخول المشبوهة أو الأنشطة الشبكية غير المعتادة)، وتوليد سردية أمنية متماسكة يمكن للقادة التعامل معها فورًا. فهي تقدم للمؤسسة **قرارات عملياتية مدروسة** بدلًا من مجرد "مؤشرات خطر"، بحيث تتضمن توصيات دقيقة: من المسؤول عن التنفيذ؟ بأي أداة؟ ضمن أي نطاق زمني؟ وما العواقب المحتملة لكل خيار؟

هذا يجعل IDSS بمثابة **العقل التنفيذي الرقمي** للمؤسسة، حيث تُدمج المعرفة التحليلية مع القدرة على التصعيد السريع، مما يُحوّل القرار من رد فعل متأخر إلى عملية مُضمنة داخل اللحظة نفسها.

**2. محركات التعلّم الآلي**(Machine Learning Engines)

تُمثل محركات التعلّم الآلي الحاسة الرقمية العميقة للمنظومة الأمنية. فهي لا تكتفي بتصنيف البيانات، بل تتعلّم باستمرار من الأنماط والانحرافات، وتبني "ذاكرة سلوكية" للتعرف على التهديدات الناشئة.

فعلى سبيل المثال، تستطيع هذه المحركات رصد تغيّر طفيف في سلوك مستخدم داخلي، أو ارتفاع غير مألوف في حجم البيانات المنقولة، أو تردد اتصالات مريب مع خوادم خارجية. بالنسبة للعين البشرية، قد تبدو هذه إشارات عادية، لكنها بالنسبة للتعلّم الآلي تمثل مؤشرات أولية للهجوم.

ومع مرور الوقت، يزداد ذكاء هذه النماذج لأنها تعيد تعريف "الطبيعي" باستمرار، وتتكيف مع تغير البيئات التشغيلية والتهديدات. بذلك، تُشكّل محركات

التعلّم خط الدفاع الأول الذي لا ينام، ويمنح المؤسسة يقظة دائمة ضد التهديدات الخفية.

### 3. تحليلات البيانات الضخمة(Big Data Analytics)

تُعد تحليلات البيانات الضخمة بمثابة العدسة الاستراتيجية الواسعة التي تمنح المؤسسة القدرة على رؤية الأنماط الكلية بدلًا من الوقائع المنعزلة. فهي تجمع بين بيانات متفرقة، كحوادث الدخول المريب، أو تراسل داخلي غير معتاد، أو حركة مرور غير طبيعية في الخوادم، لتنتج منها خريطة تهديد متكاملة.

هذه القدرة على ربط الأحداث الصغيرة في شبكة معقدة من العلاقات تُحوّل البيانات من عبء إلى قوة. فهي لا تقدم فقط "ماذا حدث؟"، بل "ماذا يعني ما حدث؟ وما التداعيات المحتملة؟ "وهكذا تتحول البيانات إلى ذخيرة معرفية قادرة على تعزيز القرارات السيادية وتقديم رؤية استباقية للخطر.

### 4. خوارزميات التوصية الأمنية المتقدمة (Advanced Security Recommendation Algorithms)

تمثل هذه الخوارزميات العقل التنبؤي للمنظومة الأمنية. فهي لا تقتصر على تحليل ما وقع، بل تولّد آلاف السيناريوهات الافتراضية وتعرضها على صانع القرار وفق احتمالات دقيقة، مدعومة بمؤشرات الثقة والتكلفة والعوائد .

ففي غرفة عمليات سيبرانية، قد تُظهر هذه الخوارزميات توصية فورية تقول: *"إذا تم عزل الخادم C الآن، ستتوقف احتمالية تسريب البيانات بنسبة 87٪، لكن ستتعطل الخدمة 6 ساعات. أما إذا تأخر القرار 3 دقائق، فاحتمالية توسع الهجوم سترتفع بنسبة 240 ".%*

هذا النوع من التوصيات لا يُقصي الإنسان من القرار، بل يُمكّنه من الحكم الواعي في لحظة الخطر، مانحًا إياه صورة مستقبلية احتمالية لا يمكن أن ينتجها الإدراك البشري وحده.

**التكامل الشبكي: الدماغ السيبراني المؤسسي**

حين تعمل هذه الأدوات مجتمعة IDSS – كقشرة تنفيذية، التعلّم الآلي كوعي باطني، تحليلات البيانات الضخمة كذاكرة استراتيجية، وخوارزميات التوصية كعقل تنبؤي – فإنها تُشكّل دماغًا سيبرانيًا مؤسسيًا يعمل بتزامن. هذا الدماغ لا يتوقف عن التعلم، ولا يترك القرار للتردد أو المفاجأة، بل يُحوّل المؤسسة إلى كيان رقمي واعٍ بذاته، قادر على التنبؤ والمناورة والتعافي.

في هذه البيئة، لا يُقاس التفوق بقدرة المؤسسة على ردع الهجمات فحسب، بل بقدرتها على هندسة القرار قبل أن تقع الأزمة .وهذا ما يجعل الذكاء الاصطناعي ليس مجرد تقنية مساعدة، بل شرطًا سياديًا يضمن بقاء القرار داخل يد الدولة أو المؤسسة، بدلًا من أن يُنتزع منها تحت وطأة الخطر.

## 3.5.نماذج القرار الاستباقيOODA Loop – Cyber Kill Chain

ونعود للتأكيد ان في بيئة السيادة السيبرانية الحديثة، لم يعد معيار نجاح القرار الأمني مرتبطًا فقط بصحته النظرية، بل بتوقيته العملي. فقد تكون الاستجابة دقيقة من حيث المحتوى والإجراءات، لكنها إذا وصلت متأخرة تحوّلت إلى عبء يرسّخ الخسارة بدلًا من منعها. وهو ما أكّد عليه المنظّر العسكري كارل فون كلاوزفيتز حين أشار إلى أن **الخطأ في التوقيت أسوأ من الخطأ في القرار** (Clausewitz, 1832/1984). هذه المقولة، التي صيغت في سياق الحروب التقليدية، تجد اليوم

صداها الأعمق في فضاء الحروب الرقمية، حيث لا يمنح الهجوم السيبراني فرصة ثانية ولا يعيد نفسه ليُراجع القادة خياراتهم.

من هذا الإدراك، برزت الحاجة إلى نماذج علمية تُعالج القرار الأمني كعملية ديناميكية مستمرة، تستبق الأحداث بدلًا من الاكتفاء برد الفعل. ومن أبرز هذه النماذج :**دورة** OODA Loop التي صاغها الطيار والمفكر العسكري الأميركي جون بويد، و**نموذج** Cyber Kill Chain الذي طورته شركة لوكهيد مارتن لتحليل وتتبع الهجمات المتقدمة.

### 3.5.1 نموذج OODA Loop سرعة الإدراك وبناء المبادرة

ابتكر **جون بويد** نموذج OODA (Observe–Orient–Decide–Act) لتحليل تفوق الطيارين في المعارك الجوية، حيث لاحظ أن الانتصار لا يرتبط دائمًا بتفوق المعدات بقدر ما يرتبط بسرعة التفكير واختصار الزمن بين الرؤية والفعل (Boyd, 1996).

في السياق السيبراني، تتحول دورة OODA إلى منظومة قرار لحظية:

- **المراقبة** :(Observe) رصد الأحداث الأمنية، سلوك المستخدمين، حركة البيانات، والمؤشرات غير المألوفة في الشبكة.
- **التوجيه** :(Orient) إعادة تفسير البيانات وفق معايير السياق المؤسسي والخبرة السابقة، مع دمج أدوات الذكاء الاصطناعي والتحليل التنبؤي لتوسيع زاوية الإدراك.
- **القرار** :(Decide) اختيار الاستجابة الأنسب، ليس فقط بناءً على البدائل، بل مع مراعاة عامل الزمن وكُلفة التأخير.

- **التنفيذ** :(Act) تطبيق القرار مباشـرة: عزل خوادم، تعطيل حسـابات، إرسـال إنذارات، أو إطلاق المسارات المضادة.

تتميّز دورة OODA بكونها حلقة متكررة وديناميكية، تتيح للمؤسسة التي تُنجزها بسـرعة أكبر من خصـمها أن تُربك المهاجم وتفرض عليه قرارات مرتجلة، وهو ما يحوّل الدفاع إلى مبادرة استباقية.

**3.5.2. نموذج Cyber Kill Chain تفكيك الهجوم عبر مراحله**

في المقابل، يركّز نموذج Cyber Kill Chain على البنية الداخلية للهجوم بدلًا من الإيقاع الزمني. وقد طوّره فريق لوكهيد مارتن كإطار لفهم وتفكيك مراحل الهجمات السـيبرانية المتقدمة. وبناء على هذا النموذج فإن الهجوم يقوم على سـبع مراحل:

1. **الاستطلاع** :(Reconnaissance) جمع المعلومات عن الأهداف والثغرات.
2. **التسليح** :(Weaponization) إعداد الحمولة الخبيثة وربطها بأداة الاستغلال.
3. **التسـليم** :(Delivery) إيصـال الهجوم عبر البريد الإلكتروني، المواقع الخبيثة أو الوسائط المحمولة.
4. **الاستغلال** :(Exploitation) تفعيل الكود الخبيث واستغلال الثغرة.
5. **التثبيت** :(Installation) ترسيخ موطئ قدم وضمان استمرارية الوصول.
6. **القيـادة والتحكم** :(Command & Control) فتح قنوات اتصـال للتحكم بالأنظمة المخترقة.

7. **تحقيق الهدف** :(Actions on Objectives) سـرقة بيانات، تخريب، أو شـنّ عمليات ابتزاز.

تكمن قوة هذا النموذج في كونه يُحوّل كل مرحلة من الهجوم إلى **فرصة لاتخاذ القرار الأمني** :فمن كشف الاستطلاع المبكر إلى تعطيل مرحلة التثبيت أو السيطرة على قنوات التحكم. وهو بذلك يحوّل الهجوم من مفاجأة صادمة إلى سلسلة قابلة للتفكيك والتعطيل.

## 3.5.3.تكامل OODA و Kill Chain من الإيقاع إلى البنية

يمثل OODA Loopو Cyber Kill Chain مدخلين متكاملين لهندسة القرار السيبراني:

- الأول يركّز على **السرعة والتوقيت** في مواجهة التهديد.
- الثاني يركّز على **تفكيك البنية والهندسة الداخلية للهجوم**.

وبينما يساعد OODA في الحفاظ على الإيقاع الاستباقي للمؤسسة، يمنح Kill Chainالقدرة على فهم نوايا المهاجم وإفشال خططه قبل اكتمالها. إن الجمع بينهما يُنتج إطارًا متقدّمًا للسيادة الرقمية، يدمج بين وعي الزمن ووعي البنية، ليعيد صياغة القرار من كونه استجابة دفاعية إلى كونه فعلًا استراتيجيًا مبادرًا .

## 3.6.تحليل المخاطر كمدخل لهندسة القرار الفعّالة.

التهديدات ليست متساوية في خطورتها. ف---الهجمات لا تحمل جميعها الأثر ذاته، ولا يمكن أن تُعالج جميعها بالآليات نفسها. ولهذا، تبدأ هندسة القرار الفعّالة من إدراك الأصول الحرجة التي تمثّل جوهر الكيان المؤسسي؛ سواء كانت

أنظمة حيوية، أو قواعد بيانات حساسة، أو حتى سمعة رقمية قد تنهار بخطأ صغير في التوقيت أو التصرّف.

لكن التهديد في البيئة السيبرانية لا يُقاس بما هو ظاهر فقط، بل بما قد يتطور إليه. فهو متغير ديناميكي يتأثر بعوامل سياسية، واقتصادية، وتقنية، وثقافية، ويتجسد في صور متعددة: من هجمات الفدية(Ransomware) ، إلى التجسس الاقتصادي، ومن الثغرات البرمجية إلى الهجمات المتعمدة على البنية التحتية الوطنية .

هنا، لا يكون القرار الجيد ردّ فعل لاحق للكارثة، بل هو فعل استباقي يُقدّر الاحتمالات قبل وقوعها، ويقيس الأثر قبل أن يُختبر بالألم. فهناك تهديدات عالية الاحتمالية ولكن منخفضة التأثير، وأخرى نادرة الحدوث لكنها كارثية من حيث النتائج. هذا ما يجعل صانع القرار أمام مفارقة استراتيجية: هل يستعد للأكثر احتمالًا، أم للأكثر تدميرًا، أم لكليهما بميزان مختلف؟

إن تحليل المخاطر هنا يتجاوز كونه مجرد أداة تنبؤية ليصبح بوصلة استراتيجية، تُمكّن القادة من ترتيب الأولويات، وصياغة السيناريوهات، وتفعيل القرارات وفق وعي عقلاني يتجاوز الارتجال والانفعال. في هذا السياق، لا يكتمل التحليل إلا إذا شمل تقييم أثر القرارات ذاتها؛ إذ قد يؤدي قرار متعجل إلى تجنب خطر آني لكنه يُدخل المؤسسة في أزمة أخرى، أو يُخفي خللًا داخليًا يُفاقم الخطر على المدى الطويل.

ومن ثمّ، يُعتبر تحليل المخاطر الحلقة الأولى في هندسة القرار السيبراني، لكنه ليس النهاية. فهو يُبنى فوقه عبر نمذجة الاحتمالات، ومحاكاة السيناريوهات، والتجارب العملية التي تمنح القرار بعدًا مركبًا يتجاوز إطفاء الحرائق إلى بناء حصون السيادة الرقمية.

وقد لخّص بيتر دراكر جوهر هذا الوعي حين قال" :ما لا يمكنك قياسه، لا يمكنك إدارته. وما لا تفهم مخاطره، لا تملك قراره .(Drucker, 1999) "هذه المقولة التي وُلدت في سياق الإدارة الكلاسيكية، تكتسب في الفضاء السيبراني بعدًا وجوديًا؛ فالغموض ليس خطرًا فقط حين يأتي من الخارج، بل حين يُولد داخل المؤسسة من عقول غير مدربة على التفكير تحت الضغط، أو من ثقافة لم تُربّ على قراءة التهديدات قبل أن تكتب فصلها الأول.

وهكذا، يتحوّل تحليل المخاطر من كونه نشاطًا إجرائيًا إلى فعل معرفي سيادي، يعيد تعريف العلاقة بين *ما نعرفه* و*ما نفتقد اليقين فيه* .فهو لا يقف عند تصنيف التهديدات، بل يطرح أسئلة وجودية: من نحن؟ ما الذي يشكّل جوهرنا الرقمي؟ وأي ثغرة قد تتحوّل من خطأ بسيط إلى انهيار شامل؟

إن المؤسسة التي تعي أصولها الحرجة وتقرأ مخاطرها بوعي، تُمارس السيادة الرقمية بمعناها الأعمق: ليس فقط عبر الحماية التقنية، بل عبر بناء ثقافة يقظة استراتيجية، تُحوّل الخوف إلى طاقة تفكير، وتحوّل الشك إلى أداة تعلم، وتحوّل الغموض إلى قرار مبني على بصيرة. ومن هنا، يُصبح تحليل المخاطر ليس فقط مدخلًا لهندسة القرار، بل الركيزة الفلسفية التي تمنحه شكله ومعناه.

فالمؤسسة التي لا تمتلك خريطة واضحة لمخاطرها هي كيان قابل للاختراق مهما بلغت استثماراتها في الأمن. أما التي تُحوّل تحليل المخاطر إلى ذاكرة مستقبلية -تُحاكي الكوارث قبل أن تقع، وتستحضر السيناريوهات قبل أن تُفرض – فإنها تُعيد صياغة علاقتها بالتهديد من موقع رد الفعل إلى موقع المبادرة. وهنا فقط يتحوّل القرار من مخاطرة إلى هندسة، ومن رد فعل إلى فعل سيادي واعٍ.

## خاتمة الفصل

عند النقطة الفاصــلة بين الخطر والاحتمال، وبين المعلومة والإدراك، تتجلى هندسة القرار السيبراني كإحدى أهم ركائز السيادة الرقمية في العصر الحديث. لم يعد القرار فعلًا إداريًا يُصــاغ في غرف مغلقة بعيدًا عن التهديدات، بل أصــبح عملية ديناميكية حيّة تتفاعل مع ضـجيج البيانات، وتُختبر في زمن شـديد السـرعة والتعقيد، حيث قد يتحول جزء من الثانية إلى فارق بين النجاة والانهيار.

أن القرار لم يعد يُقاس فقط بجودته النظرية، بل بمدى توقيته واســتباقيته. كما يقول كلاوزفيتز :الخطأ في التوقيت أســوأ من الخطأ في القرار، وهذا ما نؤكده حول نمذجة المخاطر وصــناعة القرار الاســتراتيجي. أن تجاهل الزمن المناســب يحوّل حتى أفضل القرارات إلى عبء.

وتضــمن هـذا الفصـــل أن مجـالس الإدارة لم تعـد قـادرة على إدارة الأمن الســيبراني بالأدوات التقليدية وحدها، وأنها بحاجة إلى أدوات قياس كمية ونوعية تمكّنها من رؤية المخاطر في صــورتها الكاملة. وأن النماذج التفاعلية ليســت ترفًا، بل ضرورة لإعداد المؤسسة لمواجهة ما لم يحدث بعد. هذا يتقاطع مع الدعوة الى دمج الاستخبارات التهديدية في تحليل المخاطر، بوصفها عنصرًا أساسيًا لفهم الغموض وتوجيه القرارات نحو مسارات أكثر مرونة وواقعية.

إن الذكاء الاصــطناعي لم يعد مجرد أداة مســاعدة، بل أصــبح عقلًا موازيًا لصانع القرار، يوسع أفقه ويحرره من ثقل التفاصيل. بحيث يتيح الذكاء الاصطناعي للمؤســســات التحرك من الدفاع التفاعلي إلى المبادرة الاســتباقية. وعلى الإدارات وصــانعي القرار ان يدركوا بأن جوهر الحماية في المسـتقبل هو "التصـميم الآمن منذ

البداية(Secure by Design) "، حيث لا تكون القرارات الأمنية استجابات لاحقة، بل بنى متجذرة في صلب الأنظمة.

أما على مستوى الفلسفة السيبرانية، فإن خطورة التحيزات الإدراكية التي ترافق قرارات إدارة المخاطر، مبيّنًا أن ضعف الوعي المعرفي قد يكون أشد خطرًا من ضعف البنية التحتية ذاتها. وهنا يعود صدى تحذير نيسيم طالب من "وهم القدرة على التنبؤ"، ليذكرنا أن الغاية من هندسة القرار ليست القضاء على المجهول، بل إدارة المجهول بوعي ومرونة.

وبهذا، نصل إلى خلاصة أساسية :هندسة القرار السيبراني ليست مجرد إطار تقني، بل هي فلسفة سيادية وممارسة مستمرة، تدمج العلم بالتقنية، والتحليل بالمحاكاة، والإدراك البشري بالذكاء الاصطناعي. الدولة أو المؤسسة التي لا تُحسن قراءة المخاطر قبل وقوعها، ولا تُنمذج قراراتها ضمن سيناريوهات مستقبلية، ستجد نفسها خاضعة لخيارات صاغها الآخرون.

إن السيادة الرقمية اليوم تُكتب في سطر برمجي، وتُختبر في قرار سريع، وتُترسخ في بنية معرفية مرنة قادرة على التكيّف مع ما لا يمكن التنبؤ به. وفي هذا المعنى، فإن من لا يُهندس خياراته اليوم، قد يجد نفسه غدًا ضحية خيارات لم يصنعها.

# الفصل الرابع

# الذكاء الاصطناعي في مواجهة التهديدات السيبرانية

# مقدمة الفصل

في القرن الحادي والعشرين أصبح الهجوم السيبراني حدثًا عميق الأثر يعصف بالبنى التحتية الرقمية للدول ويعيد تعريف الأمن الوطني في فضـــاء يتجاوز الحدود التقليـدية. لقـد غـدت الحروب تُدار على مســتويين متوازيين: ســـاحات الواقع، وســاحات الشــيفرة والخوارزميات، حيث يُعاد إنتاج التهديد وتشــكيل الحماية عبر أنظمة ذكية تتعلّم باستمرار.

في هذا المشـهد الجديد، يتقدّم الذكاء الاصـطناعي ليس كأداة إضـافية فحسـب، بل كبنية معرفية ناشـئة تُبشّـر بوعي دفاعي جديد. فالشـبكات العصـبية العميقة، على سبيل المثال، لا تقتصر على تخزين البيانات أو تصنيفها، بل تعيد تفسيرها لتستخرج منهـا أنمـاطًا وســـلوكيات غير متوقَّعـة. وعنـدمـا تُـدرَّب هـذه النمـاذج على رصـــد البرمجيات الخبيثة، فإنها تتجاوز حدود التصـنيف التقليدي لتطوّر قدرة شـبه حدسـية على التمييز بين السـلوك الطبيعي والسـلوك الشـاذ، بين النشـاط المشـروع والمحاولة الاختراقية.

لكن هذا التحوّل يفتح الباب أمام أسئلة سيادية وأخلاقية عميقة: إلى أي مدى يمكن الوثوق بقرارات أنظمة تتعلّم ذاتيًا؟ هل يبقى الإنســـان مالكًا لســيادته حين تصـبح الأدوات قادرة على صـياغة قراراتها بمعزل عن وعيه؟ وكيف يمكن الموازنة بين استثمار يقظة الذكاء الاصطناعي وبين الحذر من تحوّله إلى كيان غامض يصعب ضبطه؟

إنّ ما نطرحه هنا لا يقدّم الذكاء الاصــطناعي كتقنية جامدة أو خيارًا تقنيًا إضـافيًا، بل كتغيير جذري في مفهوم الحماية الرقمية. إنه دعوة إلى قراءة منطق التعلّم

الآلي باعتباره مسارًا يعيد تشكيل الأمن السيبراني على أسس جديدة: استبصار بدلًا من ردّ الفعل، وتنبؤ بدلًا من التكرار، وبناء دفاعات وطنية مرنة قادرة على الصمود أمام مستقبل لا يمكن التنبؤ بمساراته بالكامل.

### 4.1 آليات التعلّم الآلي في كشف التهديدات

يُشكّل التعلّم الآلي (Machine Learning – ML) أحد أكثر الأدوات تطورًا في مجال الدفاع السيبراني، إذ يتيح الانتقال من منطق "الاستجابة بأثر رجعي" المعتمد على قواعد وتوقيعات ثابتة، إلى منطق "الاستبصار الخوارزمي" القادر على استشراف الأنماط الشاذة قبل تحوّلها إلى تهديدات فعلية.

في الأنظمة التقليدية، كانت حلول الكشف تعتمد على التوقيعات :(Signatures)أي مقارنة كل حدث جديد بقاعدة بيانات للهجمات المعروفة. ورغم فعاليتها في مواجهة التهديدات المتكررة، فإنها عاجزة عن كشف الهجمات المتنكرة (Polymorphic Attacks)أو الهجمات الصفرية (Zero-Day Attacks) التي لا تحمل ملامح سابقة. هنا يبرز دور خوارزميات التعلّم الآلي التي تُحلل التدفقات الرقمية الضخمة وتكتشف الانحرافات الدقيقة عن السلوك الطبيعي دون الحاجة لتعريف مسبق.

#### 4.2.1 أنماط التعلّم

تقوم فعالية التعلّم الآلي على ركيزتين أساسيتين:

**أولا: التعلّم المراقب**(Supervised Learning)

يُعَدّ **التعلّم المراقب** أحد أكثر أساليب التعلّم الآلي حضورًا في ميدان الدفاع السيبراني. تقوم فكرته الجوهرية على تدريب النماذج باستخدام بيانات مصنَّفة مسبقًا، كأن تُوسَم العينة بأنها "آمنة" أو "خبيثة". ومن خلال هذا التدريب، يبني

النظام قاعدة معرفية يستند إليها في التعرّف على أنماط جديدة والتنبؤ بسلوكيات غير مألوفة.

ومن بين أبرز الخوارزميات التي أثبتت فعاليتها في هذا السياق:

- **آلات المتجهات الداعمة** :(SVMs) تُعرف بقدرتها العالية على إيجاد الحد الفاصل الأمثل بين الفئات المختلفة داخل فضاء متعدد الأبعاد. هذه الميزة تجعلها دقيقة بشكل خاص في الحالات التي تبدو فيها الفروق بين السلوكيات ضئيلة لكنّها حاسمة.
- **الغابات العشوائية** :(Random Forests) تقوم على مبدأ "التصويت الجماعي" لمجموعة من أشجار القرار، ما يمنحها قدرة أكبر على تقليل الانحياز ومعالجة الضوضاء في البيانات، وبالتالي تحقيق نتائج أكثر استقرارًا.

تجد هذه النماذج تطبيقاتها العملية في مجالات متعددة، مثل **اكتشاف البرمجيات الخبيثة** أو **تصنيف أنماط مرور الشبكات** .ومع ذلك، فإن قوة التعلّم المراقب لا تُخفي التحديات التي تعترض طريقه، إذ يظل نجاحه مرهونًا بجودة البيانات المستخدمة في تدريبه. فكلما كانت البيانات دقيقة ومتوازنة، تحسّنت كفاءة النموذج وانخفضت نسبة الإيجابيات الكاذبة؛ أما في حال غياب هذه الشروط، فقد يتحول النظام من أداة حماية متقدمة إلى مصدر إنذار مضلِّل يربك متخذ القرار.

**ثانيا: التعلّم غير المراقب**(Unsupervised Learning)

على خلاف التعلّم المراقب، يقوم **التعلّم غير المراقب** على استكشاف المجهول. هنا لا يتلقى النموذج أي وسوم مُسبقة للبيانات، بل يُترك ليستكشف بنيتها

الداخلية، فيبحث عن التكتلات الطبيعية ويعزل القيم الشـاذة. إنه بمثابة عين ثالثة ترى ما قد يعجز العقل البشري عن رصده وسط الكم الهائل من البيانات.

من أبرز تقنياته:

- **التجميع باستخدام K-Means:** حيث تُقسَّم البيانات إلى مجموعات متقاربة اعتمادًا على درجة التشابه فيما بينها. وتكمن أهميته في كشف السلوكيات غير المعتادة أو التهديدات الداخلية التي يصعب توصيفها مسبقًا.
- **التحليل إلى المكونات الرئيسية (PCA):** أداة لتقليص الأبعاد الكثيفة للبيانات، مع الحفاظ على أهم الخصائص التي تُظهر الأنماط الخفية وتُبسّط عملية الكشف عنها.

تكمن قوة التعلّم غير المراقب في قدرته على ملاحقة ما لم يُسجَّل من قبل: **التهديدات الصفرية**(Zero-Day Threats) ، أو الأنشطة التي لا تتوافق مع أي نمط معروف. غير أن هذه القوة يرافقها تحدٍ جوهري: صعوبة التفسير. فالنموذج قد يُنتج مجموعات لا تحمل معنًى أمنيًا واضحًا، ما يجعل دور المحلّل البشري حاسمًا في فهم النتائج ووضعها في سياق واقعي.

وإذا شئنا استعارة صورة ذهنية، فإن التعلّم المراقب يعمل كـ **ذاكرة الخطر**، يُعيد استدعاء ما عرفناه مسبقًا، بينما يشبه التعلّم غير المراقب **حدس المستقبل**، يستشعر ما لم يُكتشف بعد. وعندما يُدمجان معًا في نماذج هجينة، تولد أنظمة دفاعية أكثر نضجًا ومرونة: تحفظ الماضي بدقة، وتتهيأ في الوقت نفسه لمفاجآت الغد.

### 4.2.2 النماذج الهجينة والتحليل السياقي

تكمن أهمية هذه النماذج في قدرتها على قراءة السلوك الرقمي ضمن سياقه الزمني والمكاني والمؤسسي، لا باعتباره فعلًا معزولًا عن محيطه. فالملف الذي يُرسل في ساعة متأخرة من الليل، أو من موقع جغرافي غير مألوف، قد يُسجَّل كمؤشّر تهديد حتى وإن لم يتضمّن في ذاته أي محتوى ضار. إنّ القيمة هنا ليست في الحدث وحده، بل في السياق الذي يُحيط به.

لكن دور التعلّم الآلي في الدفاع السيبراني يتجاوز تحسين الأداء التقني إلى إثارة أسئلة وجودية وسيادية، تضعنا أمام معضلات غير مسبوقة:

- من يملك زمام القرار عندما تتخذ الخوارزمية إجراءً استباقيًا دون الرجوع إلى البشر؟
- هل يبقى الإنسان في موقع القيادة، أم ينزاح تدريجيًا إلى دور المراقب أمام أنظمة تتزايد استقلاليتها يومًا بعد يوم؟

هذه ليست تساؤلات نظرية بحتة، بل هي جوهر الجدل الراهن حول السيادة الرقمية والشرعية السيبرانية .فكلما ازدادت كفاءة النظم الدفاعية، تراجع التدخل البشري المباشر، مما أعاد صياغة العلاقة بين الكفاءة التقنية والشرعية السياسية والأخلاقية. وكما يشير فلوريدي وكولز، فإن مستقبل الأمن السيبراني لن يُقاس بمدى تفوقه التقني فحسب، بل بمدى قدرته على البقاء تحت مظلة القرار البشري، بحيث لا تتحوّل الخوارزميات إلى "سلطة ظلّ" تُعيد تعريف السيادة بمعزل عن أصحابها.

### 4.3 التحليل السلوكي وتحليل الأنماط(Behavioral & Pattern Analytics)

في البدايات الأولى لعلم الأمن السيبراني، وبخاصة خلال سبعينيات وثمانينيات القرن العشرين، كانت **التوقيعات الرقمية** (Signatures) هي العمود الفقري لأنظمة الكشف عن الاختراقات. كان كل هجوم يُعرَّف من خلال أثره الرقمي المميز، ثم تُقارن الأحداث الجديدة بمكتبة من التهديدات المعروفة سلفًا. وقد وصف ماثيو بيشوب هذه المرحلة، في كتابه Computer Security: Art and Science، بأنها زمن "الأمن المستند إلى الاستجابة للماضي"؛ حيث لا يتم بناء الحماية إلا على ما تم اكتشافه سابقًا.

غير أن هذه المقاربة سرعان ما واجهت حدودها مع ازدياد حجم البيانات وتعقّد أساليب الهجوم في تسعينيات القرن العشرين. عندها برزت الحاجة إلى مقاربة مختلفة لا تكتفي بالنظر إلى الماضي، بل تحاول استشعار الخطر عبر مراقبة الحاضر. وهنا لعبت دوروثي ديننغ دورًا محوريًا بطرحها لمفهوم **الكشف المستند إلى السلوك**(Behavior-Based Intrusion Detection) ، الذي يقوم على مراقبة الانحرافات عن السلوك الطبيعي للنظام بدلًا من مطابقة التهديدات المعروفة.

لقد شكّل هذا التحول نقطة انعطاف مفصلية: فبدلًا من الاقتصار على القاعدة الثابتة، أصبح الأمن السيبراني يركّز على **ما يخرج عن النمط**، أي على اللحظة التي يختلّ فيها النظام عن عادته. وهكذا وُلدت مقاربة جديدة لا تُعالج الماضي فحسب، بل تحاول أن تتنبّه إلى المستقبل.

**أولا: التحليل السلوكي**(Behavioral Analytics)

يرتكز **التحليل السلوكي** على فكرة أساسية مفادها أن لكل كيان رقمي — سواء كان مستخدمًا أو جهازًا أو تطبيقًا — **بصمة سلوكية فريدة**، وأي انحراف عنها يشكّل إشارة إنذار تستحق التوقف عندها.

ومن هذا المنطلق ظهرت أنظمة **تحليل سلوك المستخدم والكيان** (UEBA) بوصفها الامتداد المعاصر لهذا النهج. هذه الأنظمة لا تبحث في التهديدات السابقة، بل تعمل على بناء **خط أساسي للسلوك الطبيعي** (Behavioral Baseline) لكل مستخدم أو جهاز داخل المؤسسة.

وعندما يخرج الكيان فجأة عن هذا المسار المعتاد — كأن يحاول موظف الوصول إلى قاعدة بيانات حساسة لم تدخل ضمن صلاحياته من قبل، أو يقوم بعملية تسجيل دخول في وقت غير مألوف بالنسبة له — تُطلق الأنظمة إنذارًا. ليس لأن هذا الحدث مُسجَّل مسبقًا في مكتبة تهديدات، بل لأنه يمثّل **كسرًا للنمط الشخصي**، وهو ما قد يخفي وراءه نشاطًا خبيثًا أو محاولة اختراق متستّرة.

**ثانيا: تحليل الأنماط**(Pattern Analytics)

بينما يركّز **التحليل السلوكي** على الفرد أو الكيان الواحد، يذهب **تحليل الأنماط** إلى أفق أوسع، باحثًا عن التكرار والعلاقات الخفية التي تمتد عبر النظام بأكمله. فالسؤال هنا لا يكون" :*لماذا غيّر هذا المستخدم سلوكه؟* "، بل" :*هل هناك سلسلة من الأحداث تتكرر عبر كيانات متعددة وتوحي بوجود خط خفي يربط بينها؟* "

تظهر أهمية هذا النهج في رصد الظواهر التي قد تبدو عادية في صورتها الفردية، لكنها حين تتكرر أو تتقاطع تتحول إلى **إشارة استراتيجية** على وجود نشاط منسق. ومن أبرز الأمثلة:

- تكرار محاولات الدخول الفاشلة في أوقات متشابهة.
- نسخ ملفات حساسة من مواقع جغرافية متباعدة في الزمن ذاته.
- استخدام تسلسل أوامر غير مألوف يتكرر عبر عدة أجهزة.

هذه العلامات لا تعني بالضرورة وقوع خطر مباشر، لكنها غالبًا ما تشي بوجود **هجوم متدرج أو حملة منظمة**، مثل الهجمات المستمرة المتقدمة (Advanced Persistent Threat – APT). إن قوة هذا النوع من التحليل تكمن في قدرته على **جمع شظايا الأحداث الصغيرة** وتحويلها إلى صورة كلية تكشف عن سياق أكبر مما تراه العين في كل حادثة منفردة.

**ثالثا: التكامل بين التحليلين**

تكمن القوة الحقيقية للأمن السيبراني الحديث في **دمج التحليل السلوكي مع تحليل الأنماط** .فالأول يركّز على **الشذوذ الفردي**، متتبعًا ما يخرج عن النمط الطبيعي لكل مستخدم أو جهاز؛ بينما ينظر الثاني إلى **التكرار الجماعي**، باحثًا عن الروابط الخفية عبر كيانات متعددة داخل النظام.

وعندما يعمل هذان البعدان معًا، تتحول المنظومة الدفاعية إلى ما يشبه **عقلًا سيبرانيًا استقرائيًا**، قادرًا على الاستشعار المبكر للهجوم حتى قبل أن يتجسد في

صـورة تهديد صـريح. هذا التكامل لا يُضـيف طبقة تقنية فحسـب، بل يُعيد تشـكيل فلسفة الحماية ذاتها: من ردّ الفعل إلى الاستبصار، ومن المراقبة إلى الفهم.

وقد أصـبح هذا الدمج اليوم العمود الفقري لمنصـات **إدارة معلومات وأحداث الأمن** (SIEM) الذكية، مثل الأنظمة المتقدمة التي تقدمها Splunk وغيرها، والتي توظف الذكاء الاصطناعي لتحويل فيض البيانات إلى **بصيرة دفاعية** تمنح المؤسسات قدرة استباقية غير مسبوقة.

## 4.4 استخدام الشبكات العصبية العميقة في التعرف على الهجمات

تزداد تعقيدات الهجمات الحديثة مع قدرتها على **التمويه داخل حركة المرور المشـفَّرة** أو التخفي وراء تغيّرات دقيقة في الأنماط السـلوكية، بحيث تمرّ أحيانًا دون أن تلتقطها الأنظمة التقليدية. في هذا السياق، تظهر **الشبكات العصبية العميقة** (Deep Neural Networks – DNNs) كأحد أقوى الأدوات في ترسانة الدفاع السيبراني.

تقوم هذه الشـبكات على مبدأ **التعلّم التراكمي متعدد الطبقات**؛ إذ يعالج كل مسـتوى من طبقاتها البيانات بطريقة مختلفة، بدءًا من اسـتخراج السـمات البسـيطة وصولًا إلى إدراك العلاقات الأكثر تعقيدًا. هذه البنية تمنحها قدرة فريدة على **كشف الأنماط الخفية** التي قد تفلت من الخوارزميات التقليدية، والتعرّف على التهديدات الجديدة أو غير الموثقة مسبقًا.

بهذا المعنى، لا تُستخدم الشـبكات العصـبية العميقة لمجرد تحسـين الدقة في التصنيف، بل لتوسيع نطاق الرؤية الدفاعية بحيث تصبح الأنظمة قادرة على التعامل مع بيئة تتغير باستمرار، وتحتضن تهديدات لم تُكتشف بعد. إنها خطوة نحو بناء دفاع سيبراني أكثر ذكاءً، يعتمد على **الاستبصار الآلي** بدلًا من مجرد الاستجابة للمعروف.

### 4.4.1 آلية عمل الشبكات العصبية العميقة

تقوم **الشبكات العصبية العميقة** (DNNs) على مبدأ **التمثيل المتدرّج** (Hierarchical Representation)، أي بناء طبقات متعاقبة من الفهم تبدأ من البسيط وتتصاعد نحو الأكثر تعقيدًا. فالطبقات الأولى تُركّز على السمات الأساسية — مثل حجم الحزم أو نوع البروتوكول المستخدم — بينما تنتقل الطبقات الأعمق إلى تحليل العلاقات الزمنية والسلوكية المعقّدة التي قد تخفي وراءها محاولات خبيثة متطورة.

من خلال هذا التدرج، تتمكّن الشبكة من تكوين **خريطة تمثيلية داخلية** (Representation Map)للبيئة الرقمية، وهي بمثابة ذاكرة متعلّمة للنمط "الطبيعي". وعندما يظهر أي انحراف ولو كان دقيقًا، تُدرك الشبكة أن هناك شيئًا غير مألوف، ليس لأنه مسجَّل كتهديد معروف، بل لأنه لا ينسجم مع النموذج الذي بُني عبر الخبرة السابقة.

هذا التحوّل في المنطق الدفاعي يمنح DNNs قدرة عالية على اكتشاف **الهجمات غير المرئية** (Zero-Day Attacks) و**البرمجيات المتعددة الأشكال** (Polymorphic Malware)، التي غالبًا ما تفلت من الأنظمة التقليدية. وهكذا تتحوّل DNNs من مجرد أداة تصنيف إلى **نظام يقظ** قادر على استبصار التهديدات قبل أن تُعرّف رسميًا أو تُوثّق في قواعد البيانات الأمنية.

### 4.4.2 مجالات الاستخدام السيبراني

أثبتت **الشبكات العصبية العميقة** (DNNs) فعاليتها في عدة مجالات محورية ضمن الأمن السيبراني، إذ لم تعد مجرد أدوات تجريبية بل تحوّلت إلى مكوّن أساسي في استراتيجيات الحماية الحديثة. ومن أبرز تطبيقاتها:

**1. تصنيف البرمجيات الخبيثة**(Malware Classification)

تجاوزت DNNs حدود الطرق التقليدية القائمة على التوقيعات الثابتة أو السمات الشكلية للملفات. فهي تعتمد على **تحليل السلوكيات الديناميكية** والخصائص العميقة للبرمجيات أثناء التنفيذ، ما يمنحها القدرة على التعرف على البرمجيات الخبيثة **متعددة الأشكال** (Polymorphic Malware) أو تلك التي تعيد تكوين ذاتها باستمرار. بهذه الطريقة، لا تعود البنية الظاهرية للبرمجية عائقًا أمام اكتشافها، بل يصبح السلوك ذاته هو البصمة الحقيقية التي تكشف الخطر.

**2. تحليل المرور المشفَّر**(Encrypted Traffic Analysis)

يمثل المرور المشفر أحد أعقد التحديات الأمنية، إذ لا يمكن فك التشفير مباشرة لأسباب قانونية أو تقنية. ومع ذلك، تستطيع DNNs **استنتاج الأنشطة الضارة من السمات الخارجية للتدفقات الشبكية**، مثل: الأحجام الزمنية للحزم، تكرارها، وأنماط التردد. ومن دون الحاجة إلى الاطلاع على المحتوى الداخلي، تصبح الشبكة العصبية قادرة على تحديد السلوك غير الطبيعي، مما يعزز فعالية أنظمة المراقبة في البيئات عالية الحساسية مثل القطاعات المصرفية أو الحكومية.

**3. اكتشاف هجمات يوم الصفر**(Zero-Day Detection)

تعمل DNNs على بناء **نموذج للسلوك "الطبيعي** "سواء على مستوى النظام أو المستخدم. وأي انحراف عن هذا النموذج — مهما كان دقيقًا — يُفسَّر كإشارة مبكرة لاحتمالية وجود تهديد جديد. وبذلك، تُعد هذه الشبكات من أقوى الأدوات في مواجهة **هجمات يوم الصفر**، التي تمثل التحدي الأكبر للأنظمة التقليدية لأنها غير

موثقة أو معروفة مسبقًا. إن قدرة DNNs على الاستبصار تمنح المؤسسات وسيلة للتعامل مع المجهول، قبل أن يتحول إلى أزمة فعلية.

### 4.4.3 الحدود والتحديات

رغم ما تمنحه **الشبكات العصبية العميقة** (DNNs) من قدرة تحليلية عالية في مجال الكشف عن الهجمات السيبرانية، فإن تطبيقها العملي يظل محفوفًا بعدة تحديات تجعل تبنّيها الكامل في البيئات التشغيلية أمرًا معقدًا.

**أولًا: قابلية التفسير** (Interpretability)

تُعدّ القرارات الصادرة عن النماذج العميقة بمثابة *صندوق أسود*، إذ يصعب على المحللين الأمنيين تتبّع المسار المنطقي الذي قاد النموذج إلى تصنيف أو قرار بعينه. هذا الغموض لا يقتصر على كونه مشكلة تقنية، بل يثير أيضًا تساؤلات حول الثقة والشفافية، خاصة في البيئات السيادية التي تتطلب تفسيرًا واضحًا ومباشرًا لكل إجراء أمني.

**ثانيًا: الهجمات الخادعة** (Adversarial Attacks)

تواجه هذه النماذج خطر التلاعب بمدخلاتها من قِبل المهاجمين. فقد تؤدي تغييرات طفيفة جدًا — مثل تعديل بايتات محدودة في ملف أو إدخال ضوضاء بسيطة في حركة المرور — إلى خداع النموذج وإخفاء النشاط الضار. مثل هذا النوع من الهجمات يكشف هشاشة الشبكات العصبية أمام التشويش المتعمّد ويطرح تحديًا مستمرًا أمام قدرتها على الصمود.

**ثالثًا: متطلبات البيانات الضخمة** (Data Requirements)

تعتمد الشبكات العصبية العميقة على التدريب بمجموعات ضخمة ومتنوعة من البيانات. غير أن تأمين مثل هذه البيانات في المجال السيبراني يمثل تحديًا حقيقيًا، نظرًا لندرة تسجيل الهجمات الفعلية، وحساسية مشاركة البيانات بين المؤسسات، إضافة إلى القيود المتعلقة بالخصوصية. وهو ما يجعل بناء نماذج دقيقة وفعالة مهمة معقدة تتطلب موازنة دقيقة بين الحاجة إلى البيانات وحماية السرية.

## 4.5 تحديات تحيّز البيانات وشفافية القرار

يبدو الذكاء الاصطناعي، في صورته المثالية، كيانًا محايدًا: لا يغضب، لا يتحامل، ولا يُخطئ بسبب عاطفة أو نزوة شخصية. آلةٌ تُعالج الأرقام، وتُنتج القرار ببرودٍ رياضيّ يُوحي بالعدل. غير أن هذه الصورة اللامعة سرعان ما تتشقق حين نقترب من التفاصيل.

فالآلة، في حقيقتها، ليست سوى مرآة لبيئتها. هي أشبه بطفلٍ سريع التعلّم، يلتقط ما يُعرض أمامه دون نقدٍ أو تمحيص. فإذا تغذّت بياناته على واقعٍ غير عادل، فسوف يُعيد إنتاج هذا الظلم، لكن بلسانٍ رقميّ مُحايد ظاهريًا. ومن هنا تنشأ المفارقة: الذكاء الاصطناعي لا يتآمر، لكنه يكرر؛ لا ينحاز بذاته، لكنه يرث الانحياز دون وعي.

تأمل مثلًا مؤسسة مالية ضخمة تدرب أنظمتها الذكية على سنوات من سلوك الموظفين. ما تتعلمه الخوارزمية ليس "الطبيعي" في جوهره، بل "المألوف" في حدود تلك المؤسسة. فإذا انضم موظف جديد من خلفية مختلفة، يستخدم أدوات أخرى أو يعمل في أوقات مغايرة، سرعان ما تُصنّف أفعاله كمشبوهة. لم يكن تهديدًا

حقيقيًا، لكنه ببساطة لم يُشبه ما رأته الآلة من قبل. هكذا يصبح الاختلاف جريمة، ويصبح الانحراف عن المألوف دليل إدانة.

لكن الأمر لا يقف عند التحيّز وحده. فحتى حين تُصدر الآلة حكمها، نادراً ما تُفسّر السبب. تقول لك الخوارزمية: "هذا السلوك خطر"، لكنها لا تكشف كيف توصّلت إلى هذه النتيجة. تغلق الباب خلف صندوقها الأسود، وتترك البشر في مواجهة فراغ تفسيري. كما كتب فرانك باسكوال: "حين تصبح الخوارزمية سلطة لا تفسّر نفسها، فإنها لا تُصبح أكثر حيادًا، بل أكثر خطورة".

هنا يصبح الخطر مزدوجًا: ليس فقط في إمكانية الخطأ، بل في غياب القدرة على المساءلة. فإذا اعتُبر موظف بريء تهديدًا، فمن نُحاسب؟ المبرمج؟ الشركة؟ أم الكود ذاته؟ ولأن القرار صيغ بلغة رياضية باردة، فإن الاعتراض عليه يبدو ضربًا من مقاومة "العلم"، رغم أنه في جوهره مجرد تكرار لانحيازات الماضي.

لقد حذّر هانس يوناس منذ عقود من هذا المآل حين قال: "الخطر الحقيقي ليس فيما تفعله التكنولوجيا، بل فيما تفعله قبل أن نستطيع فهمه." ونحن اليوم نعيش هذا المأزق: أنظمة تتخذ قرارات أمنية حساسة قبل أن نملك القدرة على تفكيك منطقها.

إن تحيّز البيانات وغياب الشفافية ليسا مجرد مشاكل تقنية، بل قضايا سيادية وأخلاقية. فحين تتحول الخوارزمية إلى قاضٍ صامت، وحين يُصبح الكود قانونًا لا يُراجع، فإننا لا نفقد السيطرة على التقنية فقط، بل نفقد جوهر العدالة ذاته. كما قالت شوشانا زوبوف: "حين تعرف الآلة عنك أكثر مما تعرفه عن نفسك، يبدأ الحكم في التبدل من سلطة الدولة إلى سلطة الخوارزمية".

هنا يبرز السؤال الحاسم: كيف نعيد للإنسان صوته في معادلة القرار؟ كيف نضمن أن يكون الذكاء الاصطناعي أداة للحماية لا وسيلة لإعادة إنتاج التحيز؟

الإجابة لا تكمن في تحسين الخوارزميات وحدها، بل في إعادة هندسة العلاقة بين الإنسان والآلة. نحتاج إلى شفافية تُرغم النماذج على شرح قراراتها، وإلى خوارزميات قابلة للتفسير (Explainable AI) تمنح البشر القدرة على الفهم، لا مجرد الطاعة. نحتاج إلى هيئات رقابة بشرية متخصصة، تتجاوز المبرمجين لتشمل الفلاسفة، الحقوقيين، وخبراء الأخلاق. وقبل ذلك كله، نحتاج إلى الاعتراف بحق الفرد في الاعتراض على القرار الآلي، وفتح الطريق لاستئناف بشريّ يُعيد التوازن بين الكفاءة التقنية والشرعية الإنسانية.

فالذكاء الاصطناعي ليس خطرًا لأنه يفكر، بل لأنه قد يبدأ في التفكير بالنيابة عنا. والخطر الأكبر أن نستسلم لوهم حياده، ونُسلّم له زمام السيادة دون أن نملك أدوات المساءلة.

إننا بحاجة إلى ذكاء لا يكتفي بأن يتعلم، بل يعترف أيضًا بحدود معرفته. إلى أنظمة لا تُعيد إنتاج انحيازاتنا في صمت، بل تكشفها لنا بصدق. لأن المستقبل لا يُبنى على دقة بلا عدالة، ولا على كفاءة بلا وعي.

### 4.6 مقارنة بين النماذج الإحصائية ونماذج الذكاء الاصطناعي

منذ سبعينيات وثمانينيات القرن الماضي، شكّلت النماذج الإحصائية الركيزة الأولى للأمن السيبراني الناشئ. فقد بُنيت أنظمة الكشف المبكر على فرضية رياضية بسيطة: أن كل تهديد يمكن رصده حين يظهر كاستثناء عددي عن التوزيع الطبيعي. فإذا تجاوز النشاط حدود الانحراف المعياري أو خرج عن توقعات النموذج

الإحصـــائي، أطلق النظام إنذاره. كان الأمر آنذاك أشــبه بقياس النبض: أي انحراف مفاجئ عن المعدلات المعتادة يعني احتمال وجود علة تستوجب التدخل.

اعتمدت تلك المرحلة على أدوات مثل اختبار الفرضـــيات وتحليل التباين (ANOVA)ونماذج الانحدار الخطي لرصد الشذوذ. وقد وُصف هذا الاتجاه لاحقًا بأنه الكشف المستند إلى الانحراف(Anomaly-Based Detection) ؛ حيث يُعتبر أي خروج إحصائي عن "السلوك الطبيعي" مؤشّرًا على وجود تهديد. غير أن هذه الثقة في صرامة الأرقام بدأت تتزعزع مع التحولات المتسارعة في الفضاء الرقمي. فلم يعد المهاجمون يتركون أنماطًا واضحة يمكن قياسها، بل صاروا يتقنون التخفي داخل السلوك العادي، فيوزعون نشاطهم على فترات طبيعية أو يقلدون حركة مرور مألوفة بحيث لا تتجاوز أي عتبة رقمية مشبوهة. وهكذا، تحوّل الصمت الإحصائي من علامة على الأمان إلى إشارة على عجز النموذج نفسه.

مع هذا التحول، لم تعد الأساليب الإحصائية كافية. فهي بارعة في تفسير المعلوم، لكنها محدودة أمام المجهول؛ قوية في رصد الظواهر المتوقعة، لكنها عاجزة أمام التهديدات الناشئة أو هجمات يوم الصفر. ومن هنا برزت نماذج الذكاء الاصطناعي، ليس كإضافة تقنية فحسب، بل كتحوّل معرفي يغيّر طبيعة السؤال ذاته: فبينما تسأل النماذج الإحصائية "هل النشاط ينحرف عن القاعدة؟"، تسأل نماذج الذكاء الاصطناعي "ما هي القاعدة أصلًا؟" وتعيد تعريفها باستمرار.

من خلال تقنيات مثل التعلّم غير المراقب والشبكات العصبية العميقة، أصبحت الآلة قادرة على اكتشاف أنماط لم تُعرَّف مسبقًا، والتنبؤ بسلوكيات خفية لا تكشفها القياسات التقليدية. جوهر قوتها يكمن في القدرة على التكيّف مع الفوضى:

فهي لا تعتمد على فرضيات ثابتة، بل تبني إدراكها من تدفق البيانات المستمر. لكن هذه المرونة تأتي بتكلفة؛ إذ كثيرًا ما تُعتبر قراراتها بمثابة "صندوق أسود" يصعب تفسيره، وهو ما يطرح تحديات في الشفافية والثقة.

لهذا لم يعد السؤال: أيهما أفضل — الإحصاء أم الذكاء الاصطناعي؟ بل كيف يمكن الجمع بينهما؟ فقد نشأت المنظومات الهجينة (Hybrid Models) التي تجمع بين صرامة التحليل الإحصائي وديناميكية الذكاء الاصطناعي. في هذه النماذج، تعمل الخوارزميات الذكية على استشعار الشذوذات الخفية، ثم تأتي الأدوات الإحصائية لتدقق نتائجها وتتحقق من موثوقيتها. وهكذا لا يصبح القرار الأمني مجرد تنبؤ آلي، بل حكمًا يستند إلى مزيج من الاستبصار والتفسير معًا.

إن الفرق بين الإحصاء والذكاء الاصطناعي لا يعكس اختلافًا تقنيًا فحسب، بل يمثل تحولًا فلسفيًا في معنى الأمن ذاته .فبينما يرى الإحصاء الخطر كـ "انحراف عن قاعدة ثابتة"، ينظر الذكاء الاصطناعي إلى الخطر كـ "احتمال ناشئ" في بيئة متغيرة باستمرار. ومن ثم، فإن حماية المستقبل الرقمي لن تتحقق بالاعتماد على أحدهما دون الآخر، بل بالجمع بين صرامة الرقم ومرونة الاستبصار؛ بين الماضي الموثَّق والمستقبل المتخيَّل.

## خاتمة الفصل

لم يعد الذكاء الاصطناعي اليوم مجرد أداة مساعدة في ميدان الأمن السيبراني، بل أصبح عصبًا استراتيجيًا داخل منظومات الدفاع الوطني، يشارك في صياغة القرار لا في خدمته فقط. ففي الولايات المتحدة مثلًا، أتاح مشروع JADC2 لوزارة الدفاع القدرة على معالجة مليارات الحزم الشبكية في الزمن الحقيقي، ليس لاكتشاف الهجمات فحسب، بل للتنبؤ بها قبل اكتمالها؛ حتى وصف هذا التوجه بأنه محاولة لـ "كسر تسلسل الزمن "في المعركة السيبرانية.

وفي إسرائيل، أعيد تعريف مفهوم "القبة الحديدية "ليشمل الفضاء الرقمي عبر منظومة Digital Iron Dome، التي تستند إلى تقنيات التعلّم العميق لرصد الانحرافات السياقية الدقيقة في البنى التحتية الحساسة. لم تعد هذه المنظومة تنتظر الخطر ليظهر بوضوح، بل تحوّلت إلى حارس رقمي استباقي يسبق الفعل العدائي بخطوة.

أما كوريا الجنوبية، فقد صممت أنظمة دفاعية ذكية تراقب البرمجيات أثناء تشغيلها مباشرة، مما أتاح كشف الانحرافات السياقية حتى في بيئات معقدة تتضمن برمجيات متعددة الأشكال. هذه القدرة الاستباقية ساعدت على إحباط هجمات متقدمة استهدفت أنظمة القيادة والتحكم العسكرية، قبل أن تُحدث شللًا في البنية العملياتية.

وعلى الرغم من اختلاف السياقات السياسية والتقنية، فإن هذه التجارب تكشف عن مسار واحد :انتقال مركز القرار من الإنسان إلى النظام .فالآلة لم تعد تكتفي بتوصيل المعلومة أو إطلاق الإنذار، بل باتت تحدد كيفية الرد ومتى وأي درجة من

التصعيد تعتمد. هنا يظهر ما يسميه الباحثون بـ "التفويض الخوارزمي :"اللحظة التي تُمنح فيها الخوارزمية سلطة اتخاذ قرارات ذات أبعاد سيادية وأمنية، دون أن تُفصح بالضرورة عن منطقها الداخلي.

إن هذا التحول يثير سؤالًا وجوديًا عميقًا :من يحكم حين يصبح القرار السيبراني مؤتمتًا؟ هل هو الإنسان الذي صاغ الخوارزمية، أم النظام الذي أعاد تعريف الواقع وفق منطقه الخاص؟ إننا أمام مرحلة يتراجع فيها الدور البشري إلى مراقب خارجي، بينما تتحرك الآلة في صلب القرار. وهنا نستحضر تحذير باسكوال" :العدالة لا تقوم على الكفاءة وحدها، بل على الشفافية التي تُعيد الإنسان إلى قلب القرار".

إن معركة الأمن السيبراني لم تعد مجرّد سباق على السرعة أو الدقة، بل أصبحت معركة على شرعية القرار وملكيته .وعندما نُسلم للخوارزمية سلطة تحديد الخطر والاستجابة له، نكون قد انتقلنا من مرحلة "الحماية التقنية" إلى مرحلة "القيادة السيبرانية المؤتمتة" . وهنا يتجلى التحدي الأعمق: ليس في بناء أنظمة أكثر ذكاءً فحسب، بل في ضمان أن تبقى السيادة الإنسانية حاضرة، وألا يتحوّل القانون إلى مجرد ظلّ أمام سحر الخوارزمية.

# الفصل الخامس

# السيادة الرقمية بين السياسة والتكنولوجيا

# مقدمة الفصل

لقد تغيّرت بنية السلطة نفسها: فبينما كانت الدولة سابقًا الحاكم الأوحد للمجال السيادي، صعدت كيانات جديدة (شركات التكنولوجيا العملاقة ) لتشاركها، بل وتنافسها أحيانًا، على هذا الدور. فهي لم تَعُد مجرّد مزوّدين للتقنيات، بل باتت تُنتج المعايير، وتصوغ السياسات، وتقرر ما يُسمع وما يُحجب، وما يُتداول وما يُمنع. إنها "سلطة صامتة" تؤثر دون أن تُنتخب، وتعيد تشكيل الفضاء العام بلا مساءلة.

في هذا السياق، يتحول الفضاء السيبراني إلى ساحة مواجهة جيوسياسية جديدة، حيث تُشنّ الحروب بلا جيوش مرئية، بل بأكواد خفية، وتُزعزع السيادات لا عبر الاحتلال العسكري، بل عبر التحكم بالبنى الرقمية الأساسية. وهنا تبرز قضية البيانات كمحور مركزي: من يملكها؟ من يحق له الوصول إليها؟ وهل تقاس السيادة اليوم بمن يسيطر على الأرض أم بمن يملك الخوادم والسُحب؟

لقد أصبحت السيطرة على البنية التحتية الرقمية — من الكابلات البحرية التي تمر عبر المحيطات، إلى منصات الحوسبة السحابية، إلى الأقمار الصناعية — أداة سيادية أخطر من كثير من الأدوات العسكرية. إذ يكفي أن تتوقف خدمة سحابية، أو يُعاد توجيه كابل بحري، حتى تُصاب دولة بأكملها بالشلل. ولهذا، لم تعد معركة النفوذ تقتصر على الجغرافيا الطبيعية، بل انتقلت إلى الجغرافيا المعلوماتية.

وفي قلب هذه المواجهة، يتجلى التنافس بين القوى الكبرى. فالولايات المتحدة تُحافظ على هيمنة رقمية عالمية عبر شركاتها العملاقة (Google, Meta, Amazon, Microsoft)، بينما تسعى الصين إلى بناء "إنترنت سيادي" مغلق عبر

جدار الحماية العظيم، وتطوير بروتوكولات بديلة تعكس فلسفتها في المراقبة والسيطرة. أما روسيا فقد أنشأت شبكة داخلية (RuNet) تُتيح لها العمل بمعزل عن الإنترنت العالمي. في حين اختار الاتحاد الأوروبي طريقًا تشريعيًا، أبرز تجلياته اللائحة العامة لحماية البيانات(GDPR) ، لفرض قواعده السيادية على حركة البيانات العابرة للحدود.

ورغم تنوع النماذج، فإن جوهر الصراع واحد: من يملك القرار الرقمي؟ من يضع المعايير؟ ومن يحدد القواعد التي تنظّم تدفق البيانات والوعي والمعلومات؟ إنه صراع لم يعد يُقاس بامتلاك الأرض أو الموارد الطبيعية، بل بامتلاك الكود، والخوارزمية، والبنية التي تُعيد تشكيل الوعي الجمعي.

تترافق هذه التحديات مع تصاعد الحاجة إلى تشريعات سيبرانية عابرة للحدود، تحاول أن تنظم الفضاء المشترك، لكنها كثيرًا ما تصطدم بمصالح وطنية متعارضة، وبفجوةٍ متسعة بين القوانين المحلية وسرعة التقنية العابرة للدول. ومن بين المفارقات الكبرى التي تطرحها هذا الفصل: كيف يمكن تحقيق التوازن بين الخصوصية الفردية والسيطرة الوطنية؟ هل تسود الدولة عبر حماية مواطنيها، أم عبر مراقبتهم؟ وهل تستطيع حمايتهم أصلًا، دون امتلاك أدوات التدخل العميق في حياتهم الرقمية؟

وأخيرًا، لا بد من التوقّف عند نماذج الحياد السيبراني، التي تدعو إلى فصل البنى التحتية الرقمية عن السياسات، مقابل تنامي مخاطر الاعتماد التقني الخارجي، الذي قد يحوّل دولًا بأكملها إلى كيانات مستهلكة، فاقدة للقرار، تُدار تقنيًا من الخارج وإن كانت مستقلة سياسيًا من الداخل.

إن هذا الفصل لا يقدم إجابات نهائية، بل يفتح بابًا لفهم أعمق لمعنى السيادة في زمن لم تعد تُحدده الجغرافيا، بل تشكّله التكنولوجيا.

## 5.1 صراعات السيادة الرقمية في الجغرافيا السياسية

تُعَدّ السيادة الرقمية اليوم إحدى أبرز القضايا الجدلية في النظام الدولي، حيث لم يَعُد مفهوم السيادة مقتصرًا على الأرض والحدود التقليدية، بل امتد ليشمل البنية التحتية الرقمية، والبيانات، والخوارزميات، ومنصات التكنولوجيا العالمية. لقد انتقل الصراع من السيطرة على الممرات المائية والموارد الطبيعية إلى السيطرة على تدفق البيانات والتحكّم في الفضاء السيبراني، باعتباره المجال الحيوي الجديد الذي تُمارَس فيه القوة والنفوذ.

في هذا السياق، برزت الولايات المتحدة كلاعب محوري في صياغة المشهد الرقمي العالمي، عبر توظيف شركات التكنولوجيا العملاقة مثل ( Google و Meta و Amazon و Microsoft) فهي تتحكّم في محركات البحث، وخدمات الحوسبة السحابية، ومنصات التواصل الاجتماعي، بما يمنحها اليد العليا في إدارة تدفقات البيانات وإعادة تشكيل المعرفة الرقمية على المستوى الكوني.

في المقابل، تبني الصين نموذجًا مغايرًا يقوم على مبدأ "الإنترنت السيادي"، عبر منظومة الجدار الناري العظيم (Great Firewall) وتطوير بروتوكولات ومعايير بديلة تمنحها قدرة مركزية على المراقبة والتحكم. بهذا تترجم الصين رؤيتها للسيادة الرقمية كامتداد مباشر لسيادتها الوطنية.

أما روسيا، فقد اتجهت إلى بناء شبكة سيادية داخلية تعرف باسم RuNet، صُممت لتُمكّنها من العمل بمعزل عن شبكة الإنترنت العالمية عند الضرورة. بينما

اختار الاتحاد الأوروبي طريقًا قانونيًا وتنظيميًا، معتمدًا على أدوات مثل اللائحة العامة لحماية البيانات (GDPR) التي تمنحه سلطة قانونية عابرة للحدود، وتركز على حماية خصوصية مواطنيه وتقليص هيمنة الشركات الأجنبية.

ولا يقتصر هذا الصراع على الدول، بل يمتد إلى البنى التحتية الحيوية العالمية: الكابلات البحرية التي تمرر ما يزيد على 97٪ من بيانات العالم، والأقمار الصناعية، ومراكز البيانات العملاقة التي تحتكرها دول محدودة وشركات معدودة. لقد تحولت هذه البنى من مجرد قنوات اتصال إلى ساحات للتنافس الجيوسياسي والاختراق. كما باتت الهجمات السيبرانية سلاحًا جيوسياسيًا في حد ذاتها، تُوجَّه إلى المصارف ومحطات الطاقة والمصانع، بل وإلى الوعي الجمعي للشعوب عبر التضليل الإعلامي والتدخل في الانتخابات.

هذه التحولات أعادت صياغة مفهوم السيادة ذاته. فالدولة التي تعجز عن حماية بياناتها الوطنية، أو تفقد سيطرتها على الخوارزميات التي تُشكّل وعي شعبها، تصبح مكشوفة رقميًا وخاضعة — ولو بشكل غير مباشر — لنفوذ خارجي. وهنا يطل سؤال سيادي عميق: هل تمارس الدولة سيادتها حقًا إذا كانت قراراتها السيبرانية تُصاغ في مختبرات شركات أو دول أخرى؟ وهل تبقى حرة إذا كانت *منصات الاتصال التي تربط مؤسساتها ومواطنيها تدار من كيانات عابرة للحدود؟*

وعليه، فإن صراعات السيادة الرقمية في الجغرافيا السياسية لم تعد مجرد شأن تقني أو سياسي ضيق، بل غدت معركة وجودية تُحدّد من يملك الحق في صياغة الواقع الرقمي، ومن يملك أدواته، ومن يضع شروط استخدامه. لقد أصبحت

الخريطة السياسية للعالم تُرسم اليوم ليس بالحبر وحده، بل بالكود؛ لا تُحسم فقط بالحدود العسكرية، بل تُعاد هندستها عبر الخوارزميات والمنصات الرقمية.

## 5.2 تشظّي الإنترنت وبلقنته(Internet Fragmentation and Splinternet)

تأسس الحلم الرقمي على رؤية الإنترنت كفضاء مفتوح وعابر للحدود، يُقرّب بين الشعوب ويختصر المسافات نحو مجتمع معرفي عالمي. غير أن التحولات الجيوسياسية المتسارعة وتزايد الشكوك حول حيادية عمالقة التكنولوجيا، قادت إلى تفتت هذا الحلم. بدأت ملامح واقع جديد بالظهور :إنترنت متشظٍ ومُبلقن، تتوزع فضاءاته بين دول وأنظمة وفق اعتبارات سيادية ضيقة.

يشير مفهوم تشظّي الإنترنت (Internet Fragmentation) إلى الانقسام التقني والتنظيمي للشبكة، بحيث تختلف معايير التشغيل والسياسات من دولة إلى أخرى، ما يفقدها طابعها الموحّد. أما بلقنة الإنترنت(Splinternet) ، فهي استعارة من السياسة العالمية تصف انقسام الشبكة إلى "جزر سيادية" تُدار بمنطق قومي وتخضع لرقابة مشددة.

تقف الصين في طليعة هذا الاتجاه عبر الجدار الناري العظيم، الذي يُعدّ أكبر منظومة رقابة رقمية في العالم. وبالمثل طورت روسيا شبكة RuNetالقادرة على الانفصال عن الإنترنت العالمي، فيما بنت إيران شبكتها الوطنية(NIN) ، بينما يعيش مواطنو كوريا الشمالية ضمن شبكة داخلية مغلقة بالكامل.

لكن اللافت أن هذه الظاهرة لا تقتصر على الدول السلطوية. فقد تبنّت بعض الديمقراطيات الغربية سياسات "الاستقلال السيبراني"، تحت ذريعة الأمن القومي

وحماية البيانات. الاتحاد الأوروبي مثال بارز، إذ أطلق مبادرات لبنية تحتية مستقلة للبيانات والذكاء الاصطناعي، وفرض قيودًا على شركات أمريكية داخل أراضيه.

النتيجة أن الفضاء الرقمي لم يعد واحدًا، بل أصبح فسيفساء متشظية. تحوّلت الحرية الرقمية إلى حق الدولة في التحكم، واستبدلت الخصوصية الفردية برقابة سيادية وقائية. وقد يواجه المستقبل سؤالًا جديدًا: ليس "هل لديك إنترنت؟"، بل "أي نسخة من الإنترنت تستخدم؟"

## 5.3 السيادة القانونية في مواجهة السيادة الخوارزمية

يمثل التوتر بين السيادة القانونية التقليدية والسيادة الخوارزمية أحد أعقد سمات البيئة الرقمية. ففي حين يجسد القانون الوطني إرادة الدولة، تمارس الخوارزميات التي تديرها الشركات العملاقة نفوذًا سياديًا غير معلن يتجاوز الحدود، ويعيد صياغة علاقات السلطة بوسائل غير مرئية.

تحولت البيانات إلى مورد سيادي؛ من يملكها يملك المراقبة والتحليل والتوجيه. لكن هذه البيانات، التي ينتجها مواطنو الدول، تُخزّن وتُحلل غالبًا في خوادم أجنبية لا تخضع للقوانين المحلية. هكذا تنشأ المفارقة: هل تستطيع الدولة فرض قانونها على كيان رقمي عابر للحدود؟

جاءت اللائحة العامة لحماية البيانات (GDPR) الأوروبية كخطوة لاستعادة السيطرة، إذ فرضت على أي شركة – أينما كانت – الالتزام بحماية بيانات المواطنين الأوروبيين. لكن هذا المسار القانوني اصطدم بمنطق السوق الذي تتبناه الشركات العملاقة، حيث تُعامل البيانات كـ "مورد عالمي" وتُدار وفق شروطها الداخلية.

القضية الشهيرة Schrems II عام 2020 عكست هذه المعضلة. فقد أبطلت محكمة العدل الأوروبية اتفاقية Privacy Shield مع الولايات المتحدة، معتبرة أن برامج المراقبة الأمريكية تتعارض مع مستوى الحماية الذي يضمنه GDPR. كان الحكم صدمة قانونية عابرة للحدود، وأعاد التأكيد أن القانون لم يعد وحده المرجع، بل ينازعه الكود والخوارزمية في سلطة الحكم.

وهنا يتجلى السؤال: من يحكم من؟ هل يخضع المستخدم لقانون دولته، أم لشروط المنصة التي يستخدمها؟ في عصرٍ أصبحت فيه الخوارزمية قانونًا غير مكتوب، تتبدل معادلات الشرعية والسيادة.

## 5.4 الهجمات السيبرانية كأداة صراع سيادي خفي

لم تعد الهجمات السيبرانية حوادث تقنية معزولة، بل غدت أدوات صراع سيادي .أنشأت دول عدة وحدات هجومية رسمية، تستهدف البنى التحتية الحرجة: الكهرباء، الطاقة النووية، المصارف، وحتى منصات تشكيل الرأي العام.

الهجوم الشهير Stuxnet عام 2010 كشف بداية هذا التحول؛ إذ عطّل مئات أجهزة الطرد المركزي في منشأة نطنز الإيرانية وأجّل البرنامج النووي سنوات، من دون إطلاق رصاصة واحدة. ثم جاء هجوم SolarWinds عام 2020 ليظهر هشاشة سلاسل التوريد الرقمية، بعد أن تسلل المهاجمون عبر تحديث برمجي واستخدموه لاختراق وكالات حكومية أمريكية حساسة.

هذه الأمثلة تبيّن أن السيادة لم تعد تُنتزع بالقوة العسكرية وحدها، بل يمكن إضعافها عبر الاختفاء الرقمي .الدولة التي لا تمتلك قدرات سيبرانية هجومية ودفاعية متقدمة، قد تفقد سيادتها وهي لا تشعر.

## 5.5 المعايير التقنية كبؤرة للنزاع السيادي

الصراع السيبراني لا يقتصر على الهجمات، بل يمتد إلى المعايير التقنية التي تنظّم الإنترنت والذكاء الاصطناعي وإنترنت الأشياء. أصبحت هيئات مثل الاتحاد الدولي للاتصالات (ITU) و ICANNساحات خفية للصراع الدبلوماسي، حيث تسعى القوى الكبرى لفرض رؤاها على البنية التحتية العالمية.

مشروع New IPالذي اقترحته الصين عام 2019 يُعدّ أبرز الأمثلة. فهو يقدم بنية تمنح الدول قدرة مركزية على المراقبة والسيطرة على حركة البيانات. بينما يُسوَّق المشروع كحل أمني، يرى منتقدوه أنه شرعنة للرقابة وتقويض لنموذج الإنترنت المفتوح. في المقابل، تدافع الولايات المتحدة والاتحاد الأوروبي عن فلسفة الإنترنت اللامركزي وحرية الوصول.

لا تقف المسألة عند الإنترنت وحده، بل تشمل معايير التشفير، والذكاء الاصطناعي، وبروتوكولات إنترنت الأشياء .فالمعيار التقني لم يعد قضية هندسية بحتة، بل أصبح أداة سيادية تحدد شكل النظام الرقمي العالمي وقيمه.

## 5.6 الذكاء الاصطناعي كرافعة سيادية

أصبح الذكاء الاصطناعي (AI) اليوم أحد أهم ركائز السيادة الرقمية، نظرًا لدوره المركزي في الأمن القومي، الاقتصاد، وإدارة المجتمعات .فالمعادلة واضحة : من يملك البيانات، يطوّر النماذج؛ ومن يطوّر النماذج، يصوغ القرار؛ ومن يصوغ القرار، يملك السيطرة على الاتجاهات السياسية والعسكرية.

في هذا السياق، تتصدر الولايات المتحدة والصين سباق الهيمنة. فالولايات المتحدة تعتمد على شركاتها العملاقة مثل Google DeepMindوOpenAI، بينما تبني الصين منظومة ذكاء اصطناعي سيادية عبر منصات مثل BaiduوSenseTime، مدعومة بسياسات حكومية مركزية تضمن تدفق البيانات وتوافر البنية التحتية.

لكن البعد الأخطر يكمن في **الخوارزميات السيادية للقرار** .إذ لم يعد الذكاء الاصطناعي مقتصرًا على التطبيقات المدنية، بل أصبح جوهريًا في الأنظمة الدفاعية، وتحليل المخاطر، واتخاذ القرارات في البيئات المعقدة. ومع دمج الذكاء الاصطناعي في القيادة والسيطرة العسكرية، يصبح السؤال السيادي الحاسم: هل يمكن لدولة أن تحافظ على استقلالها إذا لم تطوّر ذكاءها الاصطناعي الوطني؟ (Allen & Chan, 2017).

لقد بات الذكاء الاصطناعي **بنية تحتية سيادية من الدرجة الأولى**، ومن لا يمتلكها يظل تابعًا، مهما بلغت قوته في الميادين الأخرى. إنه لم يعد ترفًا علميًا، بل شرطًا لتمكين السيادة الوطنية في القرن الحادي والعشرين.

## 5.7 هندسة الوعي الجمعي

قد لا تكمن أخطر أشكال الصراع السيادي الرقمي في البنى التحتية التقنية أو الأطر التشريعية، بل في ذلك الحيّز الرمزي غير المرئي الذي يتسلّل إلى أعماق الإنسان :الوعي الجمعي .ففي هذا المستوى، لا تُستهدف الأنظمة المعلوماتية مباشرة، بل يُعاد تشكيل الإدراك ذاته: ما يراه الأفراد، ما يعتقدونه، وما يظنونه "واقعًا موضوعيًا."

منصات التكنولوجيا الكبرى – مثل محركات البحث وشبكات التواصل الاجتماعي – لا تفرض أفكارًا بالقوة، بل تُمارس سلطة ناعمة من خلال خوارزميات الاقتراح، وترتيب نتائج البحث، وتحديد ما يُعرض وما يُحجب. وبهذه الآليات، تُهندس البيئة الإدراكية التي تتشكل فيها المواقف السياسية، والخيارات الانتخابية، والتوجهات الثقافية.

إن خوارزمية واحدة قادرة على تضخيم قضية وتهميش أخرى، أو على تقديم حدث باعتباره "مهيمنًا" بينما تُخفي آخر أكثر أهمية خلف تدفقات المحتوى. وهكذا، يُعاد تشكيل الواقع لا عبر الأكاذيب المباشرة، بل عبر ترتيب الحقائق بطريقة تخدم أهدافًا محددة. وهذا ما أطلق عليه باحثو الإعلام مصطلح هندسة الانتباه (Attention Engineering)، أي توجيه الإدراك الجماعي من خلال التحكم في مسارات الرؤية.

خطورة هذه الآلية أنها لا تحتاج إلى أدوات دعاية تقليدية أو خطب سياسية مباشرة، بل تُمارس في صمت، عبر شاشة الهاتف المحمول، وفي لحظات التصفح اليومية. وبهذا، تتحوّل المنصة الرقمية من مجرد وسيط تقني إلى **فاعل رمزي وسيادي** يشارك في صناعة الرأي العام، ويعيد تشكيل تصورات الأفراد عن أنفسهم ومجتمعاتهم.

إنها معركة على المعنى والرمز والمعرفة، أكثر منها معركة على البنية أو القانون. فالدولة قد تُؤمّن شبكاتها وتُحكم تشريعاتها، لكنها إذا غفلت عن من يُعيد صياغة وعي مواطنيها، فإنها قد تخسر المعركة من الداخل، في صمتٍ لا يُدرك إلا بعد فوات الأوان.

ولعلّ الخطر الأعمق يكمن في أن المواطن لا يُراقَب فحسب، بل يُعاد تشكيل إدراكه دون وعي منه، عبر عمليات حسابية خفية. وهنا يتجاوز مفهوم السيادة الرقمية حدوده التقنية ليغدو سؤالًا فلسفيًا–سياسيًا:

**من يُشكّل من؟ ومن يمتلك السلطة على الصورة التي نرى بها العالم؟**

## 5.8 التنافس بين القوى الكبرى في صياغة السيادة الرقمية

يشهد المشهد الجيوسياسي المعاصر تنافسًا محتدمًا بين القوى الكبرى (الولايات المتحدة، الصين، روسيا، والاتحاد الأوروبي) على إعادة تعريف السيادة في الفضاء السيبراني. هذا التنافس لم يعد يُدار عبر السلاح التقليدي أو القوة العسكرية المباشرة، بل بات يُخاض عبر الأكواد والبروتوكولات والبنى التحتية الرقمية التي تشكّل العصب الحيوي للنظام العالمي.

### 4. الصين: نموذج "السيادة الرقمية المطلقة"

تسعى الصين إلى ترسيخ نموذج "الإنترنت السيادي" من خلال جدار الحماية العظيم (Great Firewall)، الذي يفصل المستخدمين الصينيين عن الإنترنت العالمي، ويمنح الدولة قدرة شبه مطلقة على مراقبة تدفّق المعلومات والتحكم بها. هذا النموذج يترجم رؤية بكين في بناء بيئة رقمية مغلقة تُعزز الأهداف السياسية والثقافية الوطنية، وتحدّ من التأثيرات الغربية.

### 5. الولايات المتحدة: الهيمنة عبر الشركات العملاقة

في المقابل، تواصل الولايات المتحدة ممارسة نفوذها الرقمي عبر ما يمكن وصفه بـ"الهيمنة الهيكلية"، نتيجة سيطرتها التاريخية على البنية الأساسية للإنترنت.

وتُعد شركات مثلGoogle ، Apple، Meta، و Amazonأدوات رئيسية لهذه الهيمنة، إذ تتحكم فعليًا في الحياة الرقمية لمليارات المستخدمين، وتعيد صياغة تدفّق المعلومات وفق مصالحها الجغرافية والسياسية.

### 6. الاتحاد الأوروبي: السيادة القانونية والتنظيمية

أما الاتحاد الأوروبي، فيحاول بناء موقع سيادي رقمي خاص به قائم على التشريعات وحماية الخصوصية .وقد مثلت اللائحة العامة لحماية البيانات (GDPR)خطوة رائدة في فرض سيادة قانونية أوروبية على البيانات العابرة للحدود، فيما تسعى مبادرات مثل مشروع GAIA-Xإلى تقليل الاعتماد على البنى التحتية الأمريكية، وتعزيز الاستقلالية الرقمية الأوروبية.

### 7. روسيا: الانفصال الرقمي الاستراتيجي

روسيا اختارت مسارًا يقوم على الانفصال الجزئي عن الإنترنت العالمي من خلال تطوير شبكة RuNet، القادرة على العمل بشكل مستقل في حالات الطوارئ. هذا التوجه يعكس رغبة موسكو في تحصين فضائها الرقمي من التدخلات الخارجية، وترسيخ نموذج السيادة الرقمية المغلقة.

### 8. البنى التحتية الرقمية كساحة نفوذ

تتجاوز هذه الصراعات الحدود الوطنية لتصل إلى السيطرة على البنى التحتية العالمية، مثل الكابلات البحرية التي تنقل أكثر من 97٪ من بيانات العالم(، والأقمار الصناعية التي تمثل عصب الاتصال والحوسبة السحابية. السيطرة على هذه الموارد

تمنح الدول والشركات قدرة على التحكم في تدفق المعلومات أو اعتراضها أو تعطيلها، بما يعكس بعدًا استراتيجيًا للنفوذ السيبراني.

### 9. التجسس السيبراني والهجمات العابرة للحدود

يتجلى بعد آخر في استخدام الهجمات السيبرانية كأداة جيوسياسية للتأثير على مؤسسات سيادية، أو لزعزعة الاستقرار الداخلي للدول. التدخل الروسي في الانتخابات الأمريكية عام 2016، وهجوم Stuxnet على المنشآت النووية الإيرانية، وهجوم SolarWinds عام 2020، كلها أمثلة توضح كيف أصبحت البرمجيات أدوات صراع سيادي خفي.

في هذا السياق، يتبلور اتجاهان متعارضان:

- رؤية تعتبر أن السيطرة الكاملة على البيانات والبنية الرقمية حق سيادي مشروع.
- ورؤية أخرى ترى أن هذه السيطرة تُهدد حرية الإنترنت وتؤدي إلى "بلقنته " (Splinternet)، أي تقسيمه إلى فضاءات وطنية منفصلة تفقد معه الشبكة طابعها العالمي .

### 5.9. أبعاد الصراع السيادي الرقمي

تشير أبعاد الصراع السيادي الرقمي إلى الجوانب المختلفة التي تتجلى فيها المنافسة بين الدول والقوى الكبرى في الفضاء السيبراني. هذا الصراع يتمحور حول السلطة والتأثير في الفضاء الرقمي، ويتداخل فيه البعد القانوني (كسنّ القوانين والتحكم في تدفق المعلومات)، والبعد الاقتصادي (كالعملات والاقتصاد الرقمي) ،

والبعد التقني(مثل البنى التحتية والذكاء الاصطناعي)، والبعد الثقافي والسيادي (كالتأثير على الوعي والرأي العام).

### 1. البعد القانوني

يتعلق بالسؤال الجوهري :**من يملك الحق في فرض القوانين على البيانات العابرة للحدود**؟ هل هي الدولة، أم الشركة المالكة للمنصة، أم الدولة المضيفة للخوادم؟ هذه الإشكالية تعكس التوتر بين القانون المحلي وسيطرة المنصات الرقمية العابرة للحدود .

### 2. البعد التقني

الصراع يتمحور حول السيطرة على **المعايير والبروتوكولات** :من يحدد بروتوكولات التشفير، وقواعد الوصول، والخوارزميات المنظمة لتدفق المعلومات؟ لم تعد هذه قضايا تقنية بحتة، بل أصبحت أدوات سيادة خفية.(Deibert, 2013)

### 3. البعد الاقتصادي

من يملك المنصات والبنى التحتية الرقمية يملك القدرة على جني ثمار الاقتصاد الرقمي العالمي .أما الدول التي تفتقر إلى شركات محلية قوية، فتبقى مجرد أسواق استهلاكية تنتج البيانات بينما تُستثمر القيمة المضافة خارج حدودها .

### 4. البعد الثقافي والسيادي

الأخطر يتمثل في إعادة تشكيل الوعي الجمعي عبر الخوارزميات التي تتحكم في المحتوى. فهذه الخوارزميات لم تعد ناقلة للمعلومة فقط، بل أدوات لإعادة صياغة الرأي العام والقيم والسلوكيات، وهو ما يُعيد تعريف السيادة الرمزية للدول .

## 5.10 دور الشركات التكنولوجية العملاقة في صياغة القرار السيبراني

لم يَعُد النفوذ السيبراني محصورًا في وزارات الدفاع أو الأجهزة الأمنية، بل برزت الشركات التكنولوجية العملاقة كقوى "فوق–سيادية .(Meta-sovereign actors) " هذه الشــركات لا تقدّم خدمات تقنية فحســب، بل تتحكم في بنية المعرفة والوعي العام من خلال خوارزميات الترتيب والاقتراح .

الخوارزميات التي تبدو محايدة أصبحت آليات سياسية مؤثرة :فهي تحدد ما يراه الناس وما يُقصى عنهم، وتعيد تشكيل النقاش العام، وتؤثر على اتجاهات الناخبين. وقد أثبتت حادثة Cambridge Analyticaعام 2018 أن البيانات الشـخصـية يمكن استغلالها لبناء ملفات نفسية دقيقة تُستخدم في استهداف الناخبين برسائل سياسية موجهة، مما شكّل تهديدًا مباشرًا للأنظمة الديمقراطية.

تكمن المفارقة في أن هذه الشركات تمارس سلطات تُشبه سلطات الدول – من الرقابة والتنظيم والعقاب – دون أن تخضــع لآليات مســاءلة ديمقراطية. وبذلك، أصــبح القرار الســيبراني يُصــاغ ضــمن معادلة ثلاثية جديدة :الدولة، والشــركة، والخوارزمية .وهذا يثير سؤالًا جوهريًا: هل يمكن الحديث عن سيادة وطنية في فضاء تتحكم بخوارزمياته شركات خاصة عابرة للحدود؟ .

صــراعات الســيادة الرقمية لم تعد مجرّد منافســة تقنية، بل معركة متعددة الأبعاد تشــمل القانون، والتقنية، والاقتصــاد، والثقافة. القوى الكبرى تتنافس على من يضــع القواعد ومن يشكل الوعي، فيما تلعب الشــركات التكنولوجية دورًا متزايدًا في إعادة صياغة القرار السيبراني. النتيجة هي تحول الفضاء الرقمي إلى ساحة صراع سيادي عميق، يحدد من يحكم ومن يُحكم في القرن الحادي والعشرين.

## 5.11 سياسات البيانات والتشريع السيبراني: بين الخصوصية والسيادة

منذ أن تحوّلت البيانات من أثر رقمي إلى بنية للسلطة والنفوذ، لم يعد التعامل معها شأنًا تقنيًا أو اقتصاديًا فقط، بل غدت ساحة صراع سيادي تعكس توازن القوى العالمي، وتعيد رسم العلاقة بين الدولة والمواطن والشركات. لم تعد البيانات أرقامًا في خوادم، بل امتدادًا للذات الإنسانية و"أصلًا سياديًا" يتنازع عليه كما تُتنازع الموارد الطبيعية أو الممرات البحرية .

في النموذج الأوروبي، مثّل تشريع اللائحة العامة لحماية البيانات (GDPR) إعلانًا صريحًا بأن الإنسان يملك بياناته، وأن له الحق في تقرير مصير وجوده الرقمي. المادة 17، التي نصّت على "الحق في المحو(Right to be Forgotten) "، أكدت أن البيانات الشخصية ليست ملكًا للجهة التي تجمعها، بل امتداد قانوني لهوية الفرد . هذه المقاربة القانونية لا تحمي الخصوصية فحسب، بل تعيد الاعتبار لفكرة الكرامة الرقمية كأحد أبعاد المواطنة الحديثة.

لكن على الضفة الأخرى، هناك دول ترى أن البيانات مورد أمني قومي قبل أن تكون حقًا فرديًا. وتحت ذريعة "الوقاية الاستباقية"، تُوسَّع سلطات المراقبة على حساب الحريات، لتتحول السيادة الرقمية أحيانًا إلى أداة للتحكم أكثر من كونها درعًا للحماية .وهنا تتكشف المفارقة: السيادة التي تُبنى باسم الحماية قد تُستغل لتكريس الرقابة.

وفي قلب هذا المشهد، تبرز الشركات التكنولوجية العملاقة كلاعب ثالث لا يقل نفوذًا عن الدول. فشركات مثل Googleو Metaو Amazonلم تعد مجرّد مزوّدي خدمات، بل قوى فوق-سيادية تتحكم في تدفّق البيانات وتعيد تشكيل الوعي

الجمعي بخوارزميات تحدد ما يُرى وما يُخفى. كما لخص تقرير Privacy International (2021):

"لا يُقاس النفوذ في العصر الرقمي بامتلاك الأرض، بل بامتلاك البصيرة المستخلصة من تحليل البيانات".

**يتشكل إذن مشهد ثلاثي الأبعاد:**

- الدولة تسعى لفرض سيادتها على بيانات مواطنيها.
- الشركات تمارس نفوذًا استراتيجيًا تحت مظلة السوق الحر.
- المواطن يبقى الطرف الأضعف، يكافح من أجل حقه في الخصوصية والسيطرة على أثره الرقمي.

وسط هذا التشابك، يرتفع النداء لفكرة "دستور بيانات عالمي"، يُعيد كتابة العقد الاجتماعي الرقمي بلغة الحقوق الإنسانية والسيادة الذاتية، بدلًا من أن يُترك للخوارزميات تُعيد صياغته في صمت.

لكن التحدي يتضاعف عند الانتقال إلى المستوى الدولي. فالفضاء السيبراني لا يعترف بالحدود :قد يبدأ الاختراق من سنغافورة، ويُدار من أوكرانيا، ليستهدف ألمانيا عبر خوادم أمريكية. هنا جاءت اتفاقية بودابست لمكافحة الجريمة السيبرانية (2001) كأول إطار قانوني عابر للحدود. ورغم رمزيتها، بقيت محدودة النطاق وعاجزة عن فرض إلزام عالمي واسع.

**وتظهر أزمة التشريع السيبراني في بعدين أساسيين:**

1. غياب التعريف الموحّد للجريمة السيبرانية :فما يُعتبر "قرصنة" في الغرب قد يُنظر إليه في سياق آخر كـ"مقاومة رقمية" أو ممارسة مشروعة للسيادة .
2. بطء القانون أمام سرعة التقنية :فبينما تستغرق التشريعات سنوات لإقرارها، تُنفَّذ الهجمات في ثوانٍ، حتى وصف Arlanson (2020) القانون بأنه "يمشي بأرجل من طين خلف عالم يكتب قواعده في الضوء."

وهنا يبرز سؤال فلسفي جوهري :كيف نعيد تعريف الولاية القضائية في فضاء لا تحده الجغرافيا؟ ومن يُحاسَب على هجوم عابر للقارات؟ قد لا تكفي القوانين الوطنية للإجابة، بل يقتضي الأمر بناء ميثاق سيبراني عالمي يوازن بين العدالة، الشفافية، واحترام سيادة البيانات كحق إنساني مشترك.

لكن السيادة الرقمية لا تُختزل في التشريعات، بل تمتد إلى العلاقة الدقيقة بين الخصوصية الفردية والسيطرة الوطنية. فالفصل بين "العام" و"الخاص" يتلاشى في الفضاء الرقمي، والمراقبة تصبح سيفًا ذا حدين: دولٌ توسّع الرقابة باسم الأمن القومي، وأخرى تحمي الخصوصية كمبدأ دستوري لكنها تجد نفسها مكشوفة أمام الجرائم السيبرانية.

وللخروج من هذه الثنائية، اقترح باحثو Harvard Kennedy School (2022) مفهوم "السيادة الذكية"، التي ترتكز على أربعة مبادئ:

- الشفافية الخوارزمية :حق المواطن في معرفة متى وكيف تُجمع بياناته.
- الرقابة على الرقابة :إخضاع الأجهزة الأمنية لجهات مساءلة مستقلة.

- التناسب السيادي :أن تكون المراقبة بقدر الخطر لا أكثر.
- الكرامة الرقمية :معاملة الفرد ككيان حرّ لا كبيانات خام قابلة للاستغلال.

بهذا المعنى، الخصوصية ليست مجرد حق قانوني، بل حق أنطولوجي يرسّخ حدود الذات الإنسانية ويحميها من الانكشاف المطلق .إنها خط الدفاع الأخير ضد إعادة تشكيل الفرد في الخفاء عبر خوارزميات غير مرئية.

إن النقاش حول سياسات البيانات والتشريع السيبراني يوضح أننا لسنا أمام مسألة تقنية أو قانونية فحسب، بل أمام مشروع حضاري يعيد تعريف معنى السيادة في القرن الحادي والعشرين .فالمعركة لم تعد حول من يخزن البيانات، بل حول من يشكّل الوعي من خلالها. وبين دولة تسعى لحماية سيادتها، وشركات تتجاوز الحدود بسطوتها، ومواطن يبحث عن كرامته الرقمية، يظل السؤال الحاسم مفتوحًا:

هل سنعيد كتابة العقد الاجتماعي الرقمي على أسس العدالة والشفافية والكرامة؟ أم سنترك الخوارزميات تُعيد صياغته في صمت، لتصبح السلطة بلا مساءلة، والسيادة بلا معنى؟

## خاتمة الفصل

لا بد ان نؤمن بان الأمن السيبراني لم يعد فرعًا تقنيًا مكمّلًا لأنظمة الدولة، بل أصبح الامتداد الطبيعي لسلطتها الرمزية والسيادية. فمن يتهاون في بناء بنيته الرقمية المستقلة، يجد نفسه في لحظةٍ ما مجرد كيانٍ افتراضي تُدار قراراته من الخارج، وتُراقَب بياناته دون إذنه، ويُعاد تشكيل وعيه وهو غافل عن ذلك.

فالسيادة الرقمية ليست استمرارًا خطيًّا للسيادة الكلاسيكية، بل تمثّل تحولًا جوهريًا في جوهر مفهوم السيادة ذاته:

- تحوّل في المعنى، إذ لم تعد السيادة تعني الحكم السياسي فحسب، بل القدرة على صون الذات الرقمية وحماية الهوية المعلوماتية.
- تحوّل في الأدوات، حيث لم تعد تُمارس بالقوانين وحدها، بل بالخوارزميات والبرمجيات والبيانات الكبرى.
- تحوّل في الميدان، إذ لم يعد اختبارها عند الحدود الجغرافية، بل في أعماق الشبكات ومراكز البيانات.

الدولة التي تفشل في بناء بنيتها الرقمية السيادية لا تُهدَّد فقط في أنظمتها المعلوماتية، بل في معناها وشرعيتها كفاعل مستقل .فالسيادة، في جوهرها، ليست شعارًا سياسيًا، بل قدرة على اتخاذ القرار من الداخل، دون إذن من أحد، وفي كل زمان ومجال.

لقد أصبح الأمن السيبراني اليوم ساحة مركّبة :فكرية وفلسفية، تقنية واستراتيجية . فهو من جهة ميدان صراع تتقاطع فيه المصالح والقوى الكبرى، ومن جهة أخرى

ســاحة وجودية تُختبر فيها حدود الســيادة، والهوية، والقرار. في زمنٍ لا تُدار فيه الحروب بالســلاح وحده، بل بالمعلومة التي تُســرق، وبالوعي الذي يُعاد تشــكيله، باتت الصـراعات السـيبرانية وجهًا جديدًا للهيمنة، تُمارس فيه القوة بلا إعلان، وتُعاد فيه خرائط النفوذ من خلف الشاشات لا عبر الجيوش.

وعليه، لم يعد الأمن السـيبراني مجرد سباق نحو الحماية التقنية، بل صـراع على تعريف الخطر ذاته :من يملك معايير الرصــد؟ من يقرر ما يُخفى وما يُظهر؟ ومن يُحدّد شكل الواقع الرقمي الذي تتعامل معه المجتمعات؟ فالمتحكم في البنية الرقمية لا يسيطر على البيانات فقط، بل يُعيد ترميز العالم ويُهندس إدراكنا له.

إنّ هذه التحولات تجعل من الأمن السـيبراني مسـؤولية حضـارية شـاملة تتطلب يقظة معرفية، وفطنة فلسفية، واستبصـارًا بالتحوّلات الجيوسياسـية الكبرى. فالعالم اليوم لا ينقســم فقط بين دول قوية وأخرى ضــعيفة، بل بين من يدرك طبيعة هذا الصــراع ويُبدع اســتراتيجياته، ومن يظل تابعًا للتهديدات يلاحقها دون أن يُمســك بجذورها.

إنّ نهاية هذا الفصل ليس ختامًا للمناقشة، بل دعوة للوعي السيادي الرقمي :وعي يرى في التهديدات أكثر من مجرد "أكواد خبيثة"، وعي يعتبرها أدوات هيمنة ورموزًا لصـراع على القرار، فيسـعى لبناء حصـون معرفية وفكرية، لا جدران تقنية فحسـب. ففي الفضاء السيبراني، كما في الفلسفة، من لم يطرح الأسئلة الصحيحة ضلّ الطريق، ومن لم يُدرك أن المعركة تبدأ من الفكر، وجد نفسه تابعًا في عالم تصنعه خوارزميات لا تُعنى بوجوده، ولا تُترجم لغته.

# الفصل السادس

# الأمن السيبراني في البنى التحتية الوطنية

# مقدمة افصل

تشـكّل البنى التحتية الوطنية "الجهاز العصـبي العميق" للدولة، حيث يؤدّي أي خلل في نقطة منها إلى صـدمة وجودية قد تُربك القرار السـياسـي وتُعطل وظائف المجتمع. ومن هنا، لا يُقاس الأمن السيبراني بقدرته على صدّ الهجمات فحسب، بل أيضًا بمدى قدرته على التنبؤ، والتحصين، والردّ الفعّال دون أن تفقد الدولة سيطرتها أو استقرارها.

لقد لخّص "صـن تزو" هذا المبدأ قبل قرون حين قال" :*أسـمى أشـكال الذكاء الحربي ليسـت في الانتصـار بمعركة، بل في تفكيك خطط العدو دون أن تُحمل السـيوف* .(Sun Tzu, The Art of War) "وهذا ما يفعله الأمن السـيبراني المعاصـر حين يُحبط هجومًا قبل أن يبدأ، أو يكشـف نوايا عدائية كامنة في عمق شـبكة لم تُمسّ بعد. إنه فن الحماية بلا ضـجيج، والانتصـار دون مواجهة مباشـرة، والسـيادة دون استعراض.

في العمق، لا يُقاس نجاح الهجوم السيبراني فقط بقدرته على تعطيل منشأة حيوية أو إحداث أضـرار تشـغيلية، بل بكونه إعلانًا عن فشـل مفاهيمي في إدراك أن القوة الوطنية لم تَعُد تُقاس بعدد القوانين أو النصـوص الدسـتورية، بل بمدى صـلابة الشـبكات التي تُدير نبض الدولة. إن الدولة التي لا تُحصّـن بنيتها الرقمية لا تواجه خطر الأعطال التقنية فحسـب، بل خطر أن تُقاد قراراتها من الخارج، بصـمتٍ ومن وراء الشاشات، وهي لا تدري.

لقد تغيّر ميزان السيادة: فمن لا يستطيع حماية محطات طاقته، لن يستطيع حماية دستوره. ومن لا يملك السـيطرة على شبكات مياهه، سـيعجز عن ضـبط سياساته

الاقتصادية. ومن لم يؤمّن خوارزمياته ومنظوماته الرقمية، سيجد نفسه تابعًا، يُقاد من أطراف أخرى مهما بدا مستقلًا في ظاهر سياسته.

من هنا، لم يَعُد الأمن السيبراني للبنى التحتية الوطنية مجرد "جدار حماية" تقني، بل تحوّل إلى نسيج سيادي ذكي يتداخل فيه القانون مع الخوارزمية، والجندي مع المهندس، والسياسة مع البرمجة. إنه مشروع لإعادة تعريف الدولة الحديثة: دولة لا تُقاس قوتها فقط بترسانتها العسكرية، بل بقدرتها على حماية شبكاتها الحيوية، وضمان استمرارية خدماتها الأساسية، وصيانة وعيها الجمعي من التلاعب الخفي عبر المنصات والخوارزميات.

وكما يوضح دانيال سولوف" :(Solove, 2008) *الخصوصية ليست سرًّا نخفيه، بل الحق في أن نعرّف حدود ذواتنا في عالمٍ يسعى لقياس كل شيء* ".هذا المعنى ينطبق على سيادة الدولة كذلك؛ فالسيادة لم تَعُد مرتبطة بحماية الحدود المرئية فقط، بل بصون المعنى ذاته في فضاءٍ يُعاد تشكيله بالخوارزميات، حيث يصبح الأمن السيبراني امتدادًا لوجود الدولة وشرطًا لبقائها.

## 6.1 الأمن السيبراني للبنى التحتية

لم يعد أمن البنى التحتية مجرد قضية تشغيلية تقنية، بل غدا اختبارًا صامتًا لقدرة الدولة على البقاء في عصرٍ تُدار فيه الحروب عبر الأكواد بدلًا من القذائف. فبدلًا من دويّ القنابل، قد يُطفأ التيار الكهربائي، تتوقف المضخات عن العمل، تتعطل المستشفيات، ويُشلّ قطاع النقل. بهذا المعنى تتحول الحرب السيبرانية إلى امتداد للسياسة بوسائل أخرى، كما صاغها كلاوزفيتز في مقولته الشهيرة.

البنية التحتية لم تعد مجرد أنابيب أو كابلات أو أنظمة تحكم صناعي (SCADA)، بل شبكات حيّة تتقاطع عندها الفيزياء مع المنطق، والهندسة مع القرار السيادي. وأي اختراق لهذه العقد لا يعني فقط تعطيل الخدمة، بل قد يؤدي إلى إرباك الإرادة السياسية ذاتها وإفقاد الدولة قدرتها على التحكم بمقدراتها.

تكمن خطورة الهجمات السيبرانية في أنها لا تمنح ضحاياها "ترف الانتظار". فهي تتسلل خفية: عبر تحديث برمجي عادي، أو رابط مُضلل، أو ثغرة في جهاز داخلي لم يُرصد من قبل. ولهذا لم يعد مقبولًا أن تُبنى الاستراتيجيات الدفاعية على افتراض حسن النوايا، بل على افتراض السوء .ومن هنا جاءت فلسفة انعدام الثقة (Zero Trust Architecture)، التي تقوم على مبدأ أن كل نقطة وصول هي موضع تهديد محتمل، وأن الحماية لا بد أن تكون مستمرة، متدرجة، ومتعددة الطبقات.

وليس من المستغرب أن تُجمع الأطر المرجعية الكبرى مثل NIST Cybersecurity Frameworkو ISO/IEC 27001 على أن معيار الأمن السيبراني الوطني لم يعد "الاستجابة للأحداث" بعد وقوعها، بل الوقاية والمرونة، أي بناء أنظمة قادرة على الصمود والتعافي بنفس سرعة وقوع الهجوم.

**جدول (1): مقارنة بين الأمن السيبراني التقليدي وأمن البنى التحتية السيادي**

| البُعد | الأمن السيبراني التقليدي | أمن البنى التحتية السيادي |
| --- | --- | --- |
| **المنظور العام** | حماية تقنية تركز على منع الاختراقات وتأمين الأنظمة. | فلسفة سيادية شاملة تربط الأمن بقدرة الدولة على البقاء والسيطرة على وعيها وبناها الحيوية. |

| البُعد | الأمن السيبراني التقليدي | أمن البنى التحتية السيادي |
|---|---|---|
| **المجال** | شبكات الحاسوب، الأنظمة، البيانات. | الكهرباء، المياه، النقل، الصحة، الاتصالات، الطاقة... أي الجهاز العصبي الكامل للدولة. |
| **الأدوات** | جدران نارية(Firewalls) ، مضادات فيروسات، أنظمة كشف التسلل (IDS/IPS). | استراتيجيات "انعدام الثقة (Zero Trust)"، الدفاع متعدد الطبقات، التحصين الاستباقي، الذكاء الاصطناعي التنبؤي. |
| **الهدف الأساسي** | تقليل المخاطر التشغيلية. | حماية السيادة الوطنية والقرار السياسي من الانهيار الرقمي أو التبعية التقنية. |
| **الفلسفة** | ردّ الفعل :(Reactive) الاستجابة للهجمات بعد وقوعها. | الوقاية والمرونة (Proactive & Resilient): التنبؤ بالتهديدات ومنعها قبل حدوثها مع ضمان استمرارية الخدمات. |
| **مفهوم السيادة** | غير مباشر، يُفهم ضمنيًا من خلال الحماية التقنية. | مباشر وجوهري: يُعاد تعريف السيادة بوصفها القدرة على حماية "الوجود الرقمي" للدولة. |
| **المخاطر الرئيسة** | خسارة بيانات، توقف خدمات محدودة. | شلل وطني شامل: تعطيل الكهرباء، شرب المياه، النقل، الصحة، وحتى القرار السيادي ذاته. |
| **النتيجة النهائية** | حماية تقنية جزئية. | مشروع حضاري–وجودي يحمي الدولة من التفكك في عصر تُخاض فيه الحروب عبر الأكواد. |

## 6.2 أنظمة SCADA و ICSمن أدوات التشغيل إلى أعصاب الدولة

لم تَعُد أنظمة التحكّم الصناعي (ICS) مجرد تقنيات تشغيلية تهدف إلى تحسين كفاءة المصانع أو مراقبة تدفق الطاقة والمياه، بل أصبحت اليوم الجهاز العصبي العميق للدولة الحديثة .ففي محطات الكهرباء والمياه، وفي شبكات النقل والطاقة النووية، وفي المستشفيات والمنشآت الصناعية، تعمل هذه الأنظمة بصمت على إدارة نبض الحياة، بحيث يؤدي أي خلل فيها إلى صدمة وجودية قد تُربك القرار السياسي وتُعطّل وظائف المجتمع بأكمله.

في قلب هذه المنظومة تقبع أنظمة SCADA، التي تُتيح عبر واجهات برمجية متخصصة قدرة غير مسبوقة على التحكم في تدفقات الغاز، ضغط المياه، مسارات القطارات، ودرجات الحرارة داخل الأفران الصناعية. غير أنّ هذه الأنظمة، التي صُمّمت في الأصل لتعمل في بيئات معزولة، تجد نفسها اليوم مكشوفة أمام فضاء سيبراني مترابط، بعدما أُدخلت عليها تحديثات عن بُعد وربط بالشبكات العامة دون مراعاة هشاشتها البنيوية.(Palo Alto Networks, 2025)

لقد كُشفت في السنوات الأخيرة ثغرات حرجة في العديد من منصاتSCADA ، مثل أنظمةICONICS ، التي قد تسمح للمهاجمين بتنفيذ أوامر عن بُعد أو تعطيل عمليات حيوية دون أن يشعر المشغّل .وهذا يُظهر أن الهشاشة لم تعُد تقنية فقط، بل ذهنية أيضًا :إذ ما تزال هذه الأنظمة تُدار بعقلية تشغيلية بحتة، في حين يجب التعامل معها بوصفها أصولًا سيادية لا تقل أهمية عن السلاح الاستراتيجي أو القرار السياسي.

إن أي خطأ في تحديث أو ترقية برمجية داخل هذه الأنظمة ليس مجرد خلل عابر، بل قد يتحوّل فورًا إلى أثر مادي ملموس :انفجار في محطة طاقة، انقطاع في شبكة مياه، أو شلل كامل في أنظمة النقل .

المعضلة هنا لا تكمن فقط في الثغرات، بل في الفهم السياسي لطبيعة هذه الأنظمة .فمن يظن أن ضغط الغاز مسألة هندسية بحتة، لا يدرك أن التحكم في البنى التحتية يعني التحكم في إرادة الدولة ذاتها. ومن لا يملك مفاتيح تشغيل شبكاته، لا يملك فعليًا قراره السيادي .

تؤكد الدراسات الحديثة أن الهجوم على أنظمة SCADA/ICS يُترجم مباشرة إلى أزمة سيادية .ففي تقرير أمريكي صدر عام 2024، وُثّقت هجمات سيبرانية استهدفت محطات مياه ومرافق خدمية، أدت إلى تعطيل أنظمة المعالجة، وكادت تُفضي إلى كوارث بيئية وصحية .هذا الواقع يبرهن أن الحروب لم تعد تبدأ بالقصف، بل بتعطيل الكود الذي يشغّل الحياة اليومية.

ومع تصاعد التهديدات، باتت أدوات الذكاء الاصطناعي والتعلم العميق جزءًا لا يتجزأ من حماية هذه الأنظمة. فقد أثبتت مراجعات حديثة أن النماذج القائمة على الشبكات العصبية العميقة (CNNs و LSTM) قادرة على كشف الهجمات بدقة تتجاوز 90%، خصوصًا في بيئات SCADA المرتبطة بإنترنت الأشياء، كما أصبح من الضروري توفير بيئات محاكاة واقعية (Testbeds) لتقييم قدرة الأنظمة الدفاعية على مواجهة الهجمات، وهو ما أظهرته أبحاث حديثة عبر تصميم مختبرات متكاملة لإعادة بناء بيئة SCADA بكامل تفاصيلها.

هذا الوعي المتزايد بالهشاشة دفع المجتمع الدولي إلى تطوير أطر ومعايير مثل IEC 62443، التي أصبحت المرجعية الأساسية لحماية أنظمة ICS/OT (IEC, 2024).هذه المعايير تفرض قواعد صارمة للتصميم الآمن، اختبار الثغرات، وإدارة دورة حياة الأنظمة، وتشكّل اليوم أحد أعمدة السيادة الرقمية في مواجهة التهديدات الخفية.

إنّ أنظمة SCADA و ICSلم تعُد مجرّد أدوات مساعدة لتحسين الكفاءة التشغيلية، بل غدت الأعصاب الخفية للدولة الحديثة .فهي التي تضبط تدفّق الماء والكهرباء والغاز، وتتحكم في حركة القطارات والطائرات، وتؤمّن استمرارية المستشفيات والمصانع. وأي خلل فيها، مهما بدا بسيطًا، ليس حادثًا تقنيًا عابرًا، بل زلزال سيادي يربك القرار السياسي ويمسّ شرعية الدولة ذاتها.

من هنا، لم يعد الأمن السيبراني لهذه الأنظمة خيارًا هندسيًا، بل مشروعًا وجوديًا يندمج فيه القانون مع التكنولوجيا، والسياسة مع الفلسفة السيادية. فالدولة التي لا تملك القدرة على صيانة أعصابها الرقمية، ستجد نفسها في لحظة الأزمة مجرّد كيان يُقاد من الخارج دون أن يدري.

## 6.3 دروس من الهجمات الواقعية – عندما يتحوّل التهديد إلى شلل وطني

لقد وُلدت أنظمة التحكم الصناعي (ICS) وأنظمة الإشراف والتحكم وجمع البيانات (SCADA) في زمنٍ لم تكن فيه الشبكات العامة جزءًا من المعادلة التشغيلية. صُممت لتكون مغلقة بطبيعتها، تعمل في بيئات معزولة لا تحتاج إلى الحماية الخارجية، إذ كانت الحماية مضمونة بعزلها الفيزيائي عن الإنترنت. لكن مع تسارع التحول الرقمي والاعتماد على الاتصال الشبكي، تغيّر المشهد جذريًا. فقد بدأت

هذه الأنظمة تُربط بالشبكات العامة، وتُفتح لها منافذ لإدارة البيانات عن بُعد، مما كشفها لفضاء لم تُصمّم أصلًا لتحمي نفسها داخله،

وبذلك، تحوّل ما كان مغلقًا وآمنًا بعزلته إلى هدف استراتيجي بالغ الخطورة، وأصبح ما كان محصنًا ببنيته المحدودة هشًّا بانفتاحه على شبكات خارجية معقدة. فالمسألة لم تعد تقنية فقط، بل سيادية بامتياز. فأنظمة SCADA تُعدّ القلب الصناعي النابض للدولة الحديثة :هي التي تُسيّر تدفّق الكهرباء والمياه والغاز والنقل. وإن توقفت، توقفت معها الحياة العامة. في هذه الأنظمة، لا يُقاس الزمن بمنطق بيروقراطي، بل بمنطق وجودي حاد، حيث يمكن أن تُترجم ثوانٍ قليلة من التأخير إلى كارثة وطنية.

### 6.3.1 هجوم Stuxnet لحظة تحوّل في تاريخ الحرب السيبرانية

في عام 2010، كشف باحثو الأمن السيبراني عن برمجية خبيثة غير مسبوقة، لم يكن هدفها سرقة بيانات أو ابتزاز مالي، بل إحداث تخريب مادي مباشر في منشأة صناعية محصّنة داخل دولة ذات سيادة. هذه البرمجية، التي عُرفت لاحقًا باسم Stuxnet، استهدفت أنظمة التحكم الصناعي (SCADA) لشركة Siemens في منشآت تخصيب اليورانيوم الإيرانية، عبر التحكم في أجهزة الطرد المركزي وإحداث تغييرات ميكانيكية دقيقة أدت إلى إتلاف مئات منها.

آلية الهجوم كانت بالغة الدقة: إذ عمل Stuxnet على تغيير سرعات الطرد بشكل متقطع وغير منتظم، مما سبّب اهتزازًا داخليًا وتآكلًا ميكانيكيًا تدريجيًا. وفي الوقت ذاته، كانت أنظمة المراقبة تعرض للمهندسين بيانات مضللة توحي بأن التشغيل يسير

بصــورة طبيعية، لتتحول أدوات القياس إلى أدوات خداع .وبهذا، انقلب النظام على ذاته، وأصبحت الآلة تُدمّر بنيتها الداخلية دون إطلاق أي إنذار.

وقد وصــف رالف لانغر، أحد أبرز من حلّل الكود، الهجوم بقوله:
"Stuxnet is not about espionage. It’s about sabotage. It’s a cyber weapon designed to destroy equipment in the real world. That’s a new concept."

"لا يتعلق فيروس ســتوكســنت بالتجســس. إنه يتعلق بالتخريب. إنه ســلاح إلكتروني مصــمم لتدمير المعدات في العالم الحقيقي. هذا مفهوم جديد."
(Langner, 2011, TED Talk & Briefing).

إن خطورة Stuxnet تكمن في كونه أول ســلاح ســيبراني معروف أحدث دمارًا فيزيائيًا فعليًا داخل البنية التحتية، دون أي تدخل عسكري مباشر. وقد اعتبرته مجلة Foreign Affairs "الإعلان الصـامت بأن الحرب دخلت مجالًا جديدًا "ومنذ ذلك الحين، صـار يُنظر إلى البنى التحتية الصـناعية – من محطات الطاقة إلى مرافق المياه والمستشفيات – كـ أهداف عسكرية رقمية يجب تحصينها لا مجرد تشغيلها.

الأهمية الاســتراتيجية لــــ Stuxnet تتجاوز إيران. فقد أظهر أن السـيادة لم تعد تُقاس بالجيوش أو القوانين فقط، بل بقدرة الدولة على امتلاك الكود الذي يُشــغّل بنيتها التحتية .فالهجوم أثبت أن من لا يملك برمجياته وأنظمته السـيادية، يُخاطر بأن يُقاد من الخارج عبر ثغرة صــغيرة أو تحديث صــامت. وهنا يتجلى جوهر التحول : الحرب لم تعد تُعلن، بل تُمارس عبر الشــيفرة، والعدو لم يعد بحاجة إلى اجتياح جغرافي ليعيد صياغة ميزان القوى.

والأكثر إدهاشًا أن Stuxnet لم يُكتشف إلا بعد أن أنهى مهمته، إذ عمل كــ"عمل فني متقن" لا يثير الشــبهات، ما جعله يُشــكّل نقطة اللاعودة في تاريخ أمن البنى

التحتية .لقد فتح الباب أمام عصر جديد تُخاض فيه الصراعات عبر الشيفرات لا عبر المدافع، ويُعاد فيه رسم الجغرافيا السياسية من داخل الخوادم ومراكز البيانات.

### 6.3.2 هجوم BlackEnergy

في 23ديسمبر 2015، شهدت أوكرانيا واحدة من أخطر الهجمات السيبرانية على شـــبكة كهرباء وطنية في التاريخ الحديث. فقد تمكّن مهاجمون مجهولون من اســتخدام برمجية BlackEnergy 3 لاختراق أنظمة التحكم الصــناعي (SCADA) الخاصــة بشــركات توزيع الطاقة، والســيطرة على مراكز التشــغيل، ما أدى إلى قطع الكهرباء عن أكثر من 230 ألف مواطن في واحدة من أبرد ليالي الشتاء.

لم يكن هـذا الهجوم مجرد تعطيـل تقني، بـل كـان ضـــربـة اســـتراتيجيـة للثقـة المجتمعية .ففي اللحظة التي أُطفئت فيها الأضواء، لم يُختبر فقط مدى مرونة الشبكة الكهربائية، بل أيضًا قدرة الدولة على حماية مواطنيها .في سياق جيوسياسي مشحون كالذي تعيشه أوكرانيا، كان انقطاع الكهرباء رسالة مشفّرة بلغة السيادة: من لا يملك سيطرة على أنظمته التشغيلية، قد يفقد سيطرته على حدوده.

كما عبّرت الباحثة مارغريت آتكينسون في كتابها Cyber Shock: The Invisible Battlefield: " أخطر الحروب ليســت تلك التي تُدمّر المدن، بل تلك التي تُخلخل الإحســـاس بالســيطرة. حين لا يعود المواطن متأكدًا أن دولته تُدير ما يحدث، يبدأ الانهيار من الداخل، قبل أن يصل العدو إلى الخارج.(Atkinson, 2019) ".

التحقيقات التي أجرتها فرق متخصــصـــة أظهرت أن الهجوم لم يكن لحظيًا، بل اســتُبق بعملية تجسّــس ســيبراني طويلة الأمد اســتمرت عدة أشــهر. خلالها، راقب

المهاجمون العمليات اليومية، ودرسوا كيفية استخدام أنظمة SCADA من الداخل، قبل أن يُنفّذوا الهجوم عبر إيقاف القواطع الكهربائية والتحكم في أنظمة الإمداد.

ما جعل الهجوم خطيرًا لم يكن تعقيده التقني بقدر فهمه العميق للبنية التشغيلية السيادية .فقد استخدمت برمجية BlackEnergy أدوات شائعة، واستغلت ثغرات لم تُصنّف مسبقًا كحرجة، لتتحول البساطة التقنية إلى قوة استراتيجية رمزية :كل مصباح أُطفئ كان إعلانًا عن هشاشة الدولة، وكل جهاز توقّف كان دليلًا على أن السيطرة لم تعد بيدها وحدها.

أكد BlackEnergy أن الحرب الحديثة لم تعد تُخاض عبر القنابل والصواريخ، بل عبر التحكم في الأنظمة العصبية للدولة .فاستهداف الكهرباء لم يكن مجرد عبث بالخدمة، بل إعادة تعريف موازين القوة :من يسيطر على لوحات التحكم الصناعية، يسيطر ضمنيًا على الحياة اليومية لملايين البشر، ويُعيد صياغة العلاقة بين الدولة ومواطنيها.

وقد وصفت وكالة الأمن السيبراني الأمريكية (CISA, 2021) الهجوم بأنه "نقطة تحول في إدراك مخاطر استهداف البنى التحتية الحرجة، ودليل على أن التهديدات السيبرانية يمكن أن تُحدث أثرًا جيوسياسيًا يوازي الهجوم العسكري التقليدي".

لقد أثبتت حادثة BlackEnergy أن الجبهة الجديدة ليست الحدود العسكرية، بل لوحات التشغيل الرقمية .وأن الحروب لم تعد تُعلن عبر القصف الجوي، بل عبر الظلام الذي يعمّ المدن بفعل شيفرة غير مرئية. إنها لحظة فارقة أعادت تعريف الأمن القومي، وجعلت من أمن أنظمة SCADA مسألة وجودية لا تقنية فحسب.

**المرحلة الأولى– (2013) Havex: الاستطلاع كأداة حرب**

شــكّل عام 2013 نقطة تحول مبكرة في إدراك المخاطر الســيبرانية حين ظهر Havexكجزء من حملة Dragonflyالتي قادتها مجموعة Energetic Bear، مستهدفة قطاعات الطاقة والنقل والصناعة في أوروبا وأمريكا الشمالية .

لم يكن Havex يهدف إلى التدمير المباشــر، بل اعتمد أســلوب الاســتطلاع الصــامت .عبر رســائل spear-phishingومواقع watering-hole، تســلل الكود إلى الأنظمة وركز على بروتوكول OPCالذي يربط أنظمة التحكم بالمســتشــعرات الصناعية.

القيمة الحقيقية للهجوم لم تكن فيما فعله لحظيًا، بل فيما وفره من خريطة تشــغيلية للبنية التحتية .وقد وصــفت دراســات MITRE هذا النهج لاحقًا بأنه بداية مفهوم "*الاســتطلاع بوصــفه حربًا*" (reconnaissance-as-warfare) (MITRE ATT&CK, 2020).

**المرحلة الثانية – (2016) Industroyer: من الرصد إلى التعطيل**

في ديسمبر 2016، واجهت كييف واحدة من أولى التجارب العملية لـشلّ بنية تحتية مدنية عبر البرمجيات الخبيثة .فقد اســتطاع Industroyer (CrashOverride) التعامل مباشرة مع بروتوكولات صناعية أساسية مثل:

- IEC 60870-5-101/104
- IEC 61850
- OPC Data Access

كان ذلك سابقة نوعية: برمجية خبيثة تتصرف كما لو كانت مهندسًا كهربائيًا يفتح ويغلق القواطع. تضــمنت البرمجية أيضًــا مكوّن wiper لتعطيل محاولات إعادة التشغيل اليدوية .

النتيجة كانت توقف التيار الكهربائي عن أجزاء من العاصـمة، في واقعة جسـدت أن الهجوم السـيبراني يمكن أن يهز ثقة مجتمع كامل بدولته .إذا كان Havex قد قدّم "العين" التي ترسـم الخريطة، فإن Industroyer كان "اليد" التي ضـغطت على القواطع.

**المرحلة الثالثة – (2017) Triton :استهداف أنظمة الأمان**

عام 2017، ارتقت الحرب السـيبرانية إلى مسـتوى أكثر خطورة مع ظهور (Trisis) Tritonفي إحدى المنشـآت البترولية السـعودية. اسـتهدف الهجوم أنظمة السلامة الصناعية (SIS) ، وتحديدًا وحدات( Triconex منSchneider Electric) .

الغاية لم تكن تعطيل الإنتاج فقط، بل إعادة برمجة أنظمة الإنقاذ نفسـها لتعطيل تدخلها عند وقوع الخطر. بكلمات أخرى، لم يعد الكود يهاجم الخطوط الأمامية، بل دخل إلى غرفة الطوارئ محاولًا شـلّ جهاز الأمان الأخير. وقد وصـفه تقرير Trend Micro (2018) بأنه:

*"خنجر رقمي مسموم وُجه مباشرة إلى قلب أنظمة السلامة الصناعية".*

ورغم أن خطأ برمجي حال دون نجاح الهجوم، فإن الحادثة أبرزت أن البرمجيات الخبيثة تجاوزت مرحلة اسـتهداف العمليات التشـغيلية إلى محاولة تقويض آخر خط دفاع يحمي الأرواح.

**دلالات استراتيجية للثلاثية**

- Havex (2013) : تأسـيس مبدأ أن الاسـتطلاع وجمع الوعي التشـغيلي خطوة أولى للحرب السيبرانية.

- Industroyer (2016) : إظهار القدرة على تحويل المعرفة التشـغيلية إلى قوة تعطيلية تستهدف مدنًا وبنى تحتية.
- Triton (2017) : كشف أن حتى أنظمة السلامة ليست بمنأى عن الهجوم، ما يجعل الخطر سياديًا وجوديًا.

خلال خمس سنوات فقط، انتقلت الهجمات من مراقبة صامتة إلى تعطيل واسع وصولًا إلى تهديد مباشر للحياة البشرية. تكشف هذه السلسلة أن الحرب السيبرانية تتطور كمسار تصاعدي مترابط :من رسم الخرائط، إلى الضغط على القواطع، وصولًا إلى محاولة خنق أنظمة الأمان نفسها. وهو ما يبرهن أن الكود لم يعد مجرد أداة مساعدة، بل سلاحًا استراتيجيًا قادرًا على إعادة تعريف موازين القوة والسيادة.

### 6.3.3 هجوم Colonial Pipeline (مايو 2021)

يُعتبر هجوم Colonial Pipeline في مايو 2021 من أبرز الأمثلة على كيفية قدرة هجوم سيبراني محدود في مداه التقني على إحداث تأثير استراتيجي واسع النطاق. فقد بدأت العملية باختراق حساب VPN لم يكن محميًا بمصادقة متعددة العوامل، ما مكّن مجموعة DarkSide من الوصول إلى الشبكات الإدارية (IT) الخاصة بالشركة .

ورغم أن أنظمة التحكم الصناعي SCADA لم تُصَب بشكل مباشر، إلا أن الشركة اضطرت إلى إيقاف خط الأنابيب الرئيسي احترازيًا، خوفًا من انتقال العدوى الرقمية إلى الشبكات التشغيلية (DOE, 2021). أدى هذا القرار إلى توقف إمداد ما يقارب 3 ملايين برميل من الوقود يوميًا عبر شبكة بطول 5,500 ميل، وهو ما انعكس فورًا على الأسواق. في غضون ساعات، ارتفعت أسعار البنزين بشكل

ملحوظ، واصطفت السيارات أمام المحطات في ولايات مثل فلوريدا وفرجينيا وجورجيا (Time, 2021).

إزاء هذا الوضع، أعلنت الإدارة الأمريكية حالة الطوارئ في 17 ولاية ومنطقة العاصمة، كما تدخلت وزارة الطاقة لتخفيف آثار الأزمة عبر تخفيف قيود النقل وتنسيق توزيع الوقود. وفي النهاية، دفعت Colonial فدية تُقدَّر بحوالي 75 بيتكوين (4.4 مليون دولار) لاستعادة عملياتها (Wikipedia, 2023).

تكمن أهمية هذا الحدث في أنه كشف أن نقطة ضعف في نظام إداري واحد يمكن أن تشل قطاعًا اقتصاديًا كاملاً. لقد تحوّل الهجوم إلى درس عملي حول هشاشة الاعتماد اليومي على البنية التحتية الرقمية، وأجبر الدولة على التعامل مع أزمة سيبرانية على أنها أزمة وطنية استراتيجية.

### 6.3.4 هجوم NotPetya (يونيو 2017)

يُصنَّف هجوم NotPetya، الذي وقع في يونيو 2017، كأحد أخطر الهجمات السيبرانية في التاريخ الحديث من حيث حجم التأثير والخسائر الاقتصادية. بدأ الهجوم من أوكرانيا، حيث انتشر عبر تحديث برمجي مُخترق لبرنامج محاسبة محلي يُدعى MeDoc، لكنه سرعان ما تجاوز حدود الدولة ليصيب أكثر من 60 دولة حول العالم.

لم يكن NotPetya مجرد برمجية فدية، بل أداة تخريبية متعمدة. فقد أصاب الموانئ، وشركات الشحن العالمية مثل Maersk، بالإضافة إلى المصانع، والأنظمة المصرفية، وحتى شبكات المستشفيات. وبسبب انتشاره السريع عبر بروتوكولات مثل EternalBlue، أحدث الهجوم خسائر مالية ضخمة قُدرت بما يزيد عن 10

مليارات دولار عالميًا، مما يجعله أكثر الهجمات تكلفة في التاريخ (Wikipedia, 2023).

الأهمية الاستراتيجية لـ NotPetya تكمن في أنه كشف أن الأمن السيبراني لم يعد قضية محلية، بل قضية اقتصادية عالمية. لقد بيّن أن هجومًا بدأ في منشأة محلية يمكن أن يُحدث صدعًا في التجارة العالمية وسلاسل الإمداد، تمامًا كما يحدث الزلزال في شبكة المواصلات .ومن هنا، برزت القناعة أن التهديد السيبراني أصبح تهديدًا سياديًا عابرًا للحدود.

### 6.3.5 هجوم JBS Foods (مايو 2021)

في مايو 2021، تعرضت شركة JBS Foods، وهي أكبر منتج للحوم في العالم، لهجوم فدية سيبراني أصاب أنظمتها في الولايات المتحدة وكندا وأستراليا. أدى الهجوم إلى توقف العديد من مصانع المعالجة، الأمر الذي أحدث ارتباكًا في أسواق الغذاء العالمية وأثار مخاوف من أزمة غذائية محتملة.

بحسب تقارير أمنية، دفعت الشركة فدية تُقدَّر بـ 11 مليون دولار بالبيتكوين من أجل استعادة السيطرة على أنظمتها (Wikipedia, 2023). لم يكن هذا الهجوم مجرد حدث تقني، بل كان رسالة استراتيجية تؤكد أن الأمن الغذائي نفسه أصبح جزءًا من ميدان الحرب السيبرانية.

إن ما يجعل هجوم JBS مميزًا هو طبيعته الرمزية: لم يكن الهدف تعطيل الكهرباء أو المال، بل ضرب عنصر أساسي من عناصر الحياة اليومية، وهو الغذاء. لقد أظهر أن التهديد السيبراني يمكن أن يتسلل إلى تفاصيل الحياة الصغيرة للأفراد، من المائدة إلى محطة الوقود.

### 6.3.6 هجمات ShadowGrid (2022)

في عام 2022، رُصدت موجة من الهجمات السيبرانية المتفرقة التي استهدفت شبكات Smart Grids في عدة دول أوروبية. هذه الشبكات تُعتبر العمود الفقري لأنظمة الطاقة والمياه الحديثة، إذ تعتمد على تقنيات التشغيل الذكية في التوزيع والتحكم اللحظي.

ما يميز هذه الهجمات هو أنها لم تُعلن كأحداث عدائية واضحة، بل جرى التعامل معها غالبًا تحت غطاء "اختبارات جاهزية". هذا الوصف يحمل دلالتين: الأولى أنه محاولة لطمأنة الجمهور، والثانية إقرار ضمني بأن التهديد بات واقعيًا لدرجة يتطلب معها إدارة تكتمية.

بذلك، لم يعد الهجوم السيبراني يُعرَّف كـ "حرب صريحة"، بل تحوّل إلى حالة اختبارية صامتة. حيث أصبحت الدول ميدانًا لتجارب الخصوم، لا لرؤية قدرتها على الصمود بعد الضربة، بل لرصد كيفية استجابتها عندما يُلمَّح لها بالضربة فقط.

هذا التحول يوضح أن السيادة الرقمية لم تعد تُقاس بالحدود الجغرافية أو حتى بالأنظمة المركزية، بل بقدرة الدولة على حماية أكوادها التشغيلية الدقيقة، لأن اختراقها قد يعادل اختراق جسدها الوطني ذاته.

## 6.4 الدفاع الذكي: فلسفة الحماية في عمقها.

خلال العقدين الأخيرين شهدت الفلسفة الدفاعية في المجال السيبراني تحوّلًا جذريًا؛ إذ انتقلت من منطق **الوثوق المسبق** إلى منطق **الشك التأسيسي** .فبينما افترضت الأنظمة التقليدية أن الخطر يأتي من الخارج وأن الداخل آمن بطبيعته، كشفت التجارب الحديثة أن التهديدات الداخلية – سواء المتعمدة Insider)

(Threatsأو الناتجة عن الإهمال – لا تقل خطورة عن التهديدات الخارجية . وبذلك، لم تعد الحماية تعني غياب الهجوم مؤقتًا، بل اليقظة المستمرة تجاه احتماله.

### 1. فلسفة الدفاع الذكي

من هذا التحوّل ولدت فلسفة الدفاع الذكي(Intelligent Defense) ، التي لا تُختزل في بناء جدران تقنية أو أنظمة تقليدية، بل ترتكز على هندسة العمق الأمني عبر كل طبقة من طبقات البنية التحتية، البشرية والتقنية معًا. الفكرة الجوهرية هنا أن الثقة لم تعد قاعدة بل استثناء؛ فكل دخول، وكل تبادل بيانات، وكل حركة داخل الشبكة تُعامل بوصفها حدثًا يستدعي التحقق المستمر، وهو ما يمثل الانعطافة الكبرى في العقلية الدفاعية الحديثة.

### 2. نموذج "انعدام الثقة(Zero Trust "

يُعد Zero Trust أحد الأعمدة المركزية لهذه الفلسفة. وقد عرّفته الوكالة الأمريكية للأمن السيبراني والبنية التحتية (CISA) بأنه "نموذج لا يمنح أي كيان ثقة ضمنية، بل يفرض التحقق المستمر لكل مستخدم وجهاز وتطبيق.(CISA, 2021) " وتقوم فكرته على أن كل عملية وصول يجب أن تُعتبر تهديدًا محتملًا حتى يثبت العكس، وذلك عبر التحقق من:

- هوية المستخدم.(Identity)
- حالة الجهاز.(Device Health)
- السياق المكاني–الزماني.(Context)

- التحليل السلوكي مقارنةً بالسجل التاريخي.(Behavioral Analytics)

وقد أثبتت الدراسات أن اعتماد Zero Trust يقلل الحوادث السيبرانية بما يصل إلى 70٪ في العام الأول من تطبيقه.(Microsoft, 2022)

3. **نموذج "الدفاع في العمق(Defense in Depth) "**

يقوم Defense in Depthعلى مبدأ الحصون القديمة: الحماية ليست جدارًا واحدًا بل سلسلة طبقات متداخلة. ووفق تعريفNIST ، هو "إستراتيجية أمنية توزّع طبقات متعددة من الضوابط بحيث يمكن لكل طبقة أن تعوّض قصور الأخرى "

**ويهدف هذا النهج إلى:**

- إبطاء المهاجم وإجباره على مواجهة عدة عوائق متتابعة.
- كشف التهديد مبكرًا عبر مراقبة نشاطات مشبوهة في أكثر من نقطة.
- منح الوقت للفِرق الأمنية كي تستجيب وتحتوي الهجوم.

ومن الأمثلة البارزة اختراق **شركة** Target **الأمريكية عام 2013**، الذي بدأ عبر ثغرة في بيانات الموردين. لو كانت طبقات متعددة من الضوابط مطبّقة، لكان بالإمكان احتواء الهجوم قبل وصوله إلى بيانات العملاء.

**4. العقل الأمني الجديد: فلسفة الشك البنّاء**

ما يميز هذا التحول هو بروز ما يمكن تسميته بـ العقل الأمني الجديد، الذي ينتقل من سؤال :من أثق به؟ إلى سؤال :كيف أتحقق دائمًا؟.

التحقق هنا لا يعني الارتياب المرضـي، بل بناء أنظمة يكون التحقق فيها عملية طبيعية متواصلة وليست استثناءً. وكما قال ديكارت: "أنا أشك، إذًا أنا موجود"، فإن المنطق الدفاعي الجديد يقول: "أنا أتحقق، إذًا أنا آمن.(Forrester, 2021) " هكذا يتحول الشك من نفي للثقة إلى إطار منهجي للوعي الأمني، حيث تراجع كل طبقة أمنية الطبقة الأخرى، ويُعاد فحص كل عملية حتى لو بدت مألوفة، فيتحول العمق الأمني إلى بنية معرفية بقدر ما هو بنية تقنية.

### 6.5 هندسة الدفاع الذكي: من المفهوم إلى التطبيق

لا يقتصر الدفاع الذكي على الأدوات، بل هو **فلسفة متكاملة** تُحوّل البنية التحتية الرقمية إلى جهاز عصبي واعٍ قادر على الاستشعار المبكر والتفاعل الديناميكي مع التهديدات. ويتجسد هذا النهج في تقنيات متقدمة مثل:

1. **أنظمة إدارة معلومات وأحداث الأمن:(SIEM)** تُعدّ الأنظمة الذكية مثل Splunk حجر الأساس في مراقبة البيئات الرقمية المعقدة، إذ تقوم بجمع السجلات من مصادر متعددة وتحليلها للكشف عن الأنماط الشاذة والتهديدات المحتملة.

2. منصات **الكشف والاستجابة الممتدة:(XDR)** تمنح هذه المنصات رؤية موحّدة تغطي كامل البيئة الرقمية، من النقاط الطرفية إلى البنى السحابية، مما يعزز من سرعة الاستجابة ودقة القرار الأمني.

3. التحقق **السياقي متعدد العوامل**: لم يعد التحقق من الهوية يعتمد على كلمة المرور وحدها، بل أصبح يرتكز على دمج العوامل المتعددة (MFA) مع السياق التشغيلي للمستخدم — مثل الموقع الجغرافي أو وقت الدخول — لتقليل احتمالية الانتحال أو الوصول غير المشروع.

4. **التحليل السلوكي المدعوم بالذكاء الاصطناعي**: تسمح هذه التقنية برصد الانحرافات الدقيقة في سلوك المستخدم أو النظام، عبر بناء خط أساس للسلوك الطبيعي ثم اكتشاف أي خروج عنه. وقد أصبح هذا النهج عنصرًا أساسيًا في الأطر المرجعية العالمية مثل.(MITRE (MITRE, 2020

أما فلسفيًا، فإن Zero Trust وDefense in Depth لا يمثلان مجرد نماذج تقنية، بل **نقلات فكرية** في مقاربة الأمن: حيث تتحول الحماية من جدار ساكن إلى شبكة من الأسئلة والاختبارات، ومن رد فعل إلى ممارسة واعية للشك والتحقق.

في جوهرها، تعني فلسفة الدفاع الذكي **القدرة على احتواء الأسوأ قبل أن يولد**، وتجسيد الفكرة بأن السيادة الرقمية ليست إعلانًا رسميًا، بل ممارسة يومية متجددة، يتداخل فيها الوعي الأمني مع القرار السيادي في علاقة جدلية لا تنفصم.

## 6.6 مقارنة بين استراتيجيات الاستجابة السيادية: دروس من إستونيا، سنغافورة، والإمارات

أصبحت الهجمات السيبرانية لحظات كاشفة لبنية القرار والسيادة الرقمية. بعض الدول حولت هذه الأزمات إلى فرص لإعادة بناء أنظمتها على أسس أكثر وعيًا واستباقًا. من أبرز هذه التجارب: إستونيا، سنغافورة، والإمارات، حيث اختلفت المسارات لكنها التقت عند فكرة محورية: أن القرار السيادي لا يُمارس عند وقوع الهجوم فقط، بل يُزرع مسبقًا في التعليم، التشريع، والتصميم المؤسسي.

### 6.6.1 إستونيا: من الصدمة إلى تأسيس الهوية السيبرانية

عام 2007، تعرضت إستونيا لهجوم سيبراني واسع أصاب وزاراتها، بنوكها، وخدماتها الحيوية. ورغم أن الحدث اعتُبر كارثة وجودية في حينه، فقد شكّل نقطة

تحوّل جذري نحو بناء هوية سـيبرانية متكاملة. قامت إسـتونيا بإنشـاء مركز الدفاع السـيبراني التعاوني للناتو(CCDCOE) ، ما منحها دورًا دوليًا مرجعيًا في صـناعة الفكر السـيبراني. كما أسسـت نظام الهوية الرقمية الوطنية (e-ID) الذي أعاد تعريف علاقة المواطن بـالـدولـة عبر تمكينـه من التحكم ببيانـاتـه والتفاعـل مع الحكومـة بـأمـان وشفافية وأخيرًا، بلورت الدولة ما يُعرف بـ"العقد الرقمي الاجتماعي"، حيث أصبح الحق الرقمي امتدادًا طبيعيًا للحق الدسـتوري، مما حوّل إسـتونيا إلى نموذج رائد عالميًا في مفهوم الدولة السيبرانية.

### 6.6.2 سنغافورة: الحوكمة كوقاية سيبرانية

على عكس إسـتونيا، لم تنتظر سـنغافورة أزمة كبرى لتعيد التفكير بأمنها السيبراني، بل اختارت الوقاية المُمأسسة. أنشأت وكالة الأمن السيبراني (CSA) كهيئة مستقلة ذات صلاحيات تشريعية وتنفيذية، لتقود القرار السيبراني من موقع التوجيه لا الاستجابة. اعتمدت الدولة استراتيجية وطنية تقوم على ثلاثة ركائز: التعليم، البحث العلمي، والشـراكـات الـدوليـة، إدراكًا بـأن الأمن لا يُبنى بـالجـدران بـل بـالوعي والقدرات البشرية. كما تبنّت نموذج الأنظمة المعزولة (Air-Gapped Systems) في البنى التحتية الحسـاسـة، ما يعكس فلسـفة "الشـك البنّاء" التي تفترض دائمًا احتمال الاختراق وتمنع آثاره بنيويًا. بهذه السياسات، صار القرار السيبراني في سنغافورة جزءًا من الثقافة المؤسسية، لا مجرد وظيفة تقنية.

### 6.6.3 الإمارات: الابتكار كأداة سيادية

أما الإمارات، فقد اختارت مسـارًا ثالثًا يقوم على دمج الأمن السـيبراني في مشـروع التحول الرقمي الوطني بأكمله. أُنشـئت الهيئة الوطنية للأمن السـيبراني

بصـلاحيات تشـريعية وتنفيذية، لتؤدي دور "المهندس السـيادي" للفضـاء الرقمي UAE .كما دمجت الدولة الأمن السيبراني في تصميم جميع المشاريع الحكومية منذ البداية، لتصـبح الحماية خاصـية متأصـلة وليسـت وظيفة لاحقة. وعلى مسـتوى الابتكار، استثمرت الإمارات في مختبرات المحاكاة وحاضنات التهديدات Cyber) (Rangesالتي تُدرّب الكفاءات على مواجهة سـيناريوهات افتراضـية للهجمات، بما يعزز الاسـتعداد الاسـتباقي .(Al-Khouri, 2020) وهكذا، لم يعد القرار السـيبراني مجرد رد فعل، بل ممارسة يومية للجاهزية والوقاية الذكية.

### 6.6.4 تكشف التجارب الثلاث عن ثلاث مقاربات متكاملة لبناء السيادة الرقمية:

- إستونيا :السيادة تولد من الأزمة عبر إعادة بناء الدولة على أسس رقمية.
- سنغافورة :السيادة تتحقق عبر الوقاية والحوكمة المستمرة.
- الإمارات :السيادة تُصنع بالابتكار ودمج الأمن في كل مسار للتحول الرقمي.

المشـترك بينها هو أن الأمن السـيبراني لم يعد مجرد أداة تقنية، بل بنية معرفية وسياسية، تتحقق من خلال القدرة على التوقع، التصميم، والتعلم المؤسسي.

لقد أثبتت هذه التجارب أن السـيادة الرقمية ليسـت حالة طارئة تُسـتدعى عند الأزمات، بل هي ممارسـة مسـتمرة تُصـاغ في بنية الدولة منذ التأسـيس. فالهجوم السـيبراني لم يعد يُنظر إليه كخلل أمني عابر، بل كمرآة تكشـف عن عمق الدولة في إدراكها لمواضع قوتها وضعفها، وعن مدى نضج فلسفة القرار فيها.

في إستونيا، وُلدت السيادة من قلب الأزمة؛ حيث تحوّلت لحظة الانكشاف عام 2007 إلى نقطة انطلاق لإعادة بناء الدولة ككيان رقمي متكامل، يقوم على الهوية

الإلكترونية، والعقد الرقمي الاجتماعي، والريادة الدولية في الدفاع السيبراني. أما سنغافورة فقد اتخذت مسارًا وقائيًا واعيًا، إذ صاغت القرار السيبراني كجزء من منظومة الحوكمة ذاتها، فبنت وكالة متخصصة، ورسّخت التعليم والبحث والشراكات الدولية، لتجعل الأمن ممارسة جماعية متوزعة لا تنتظر صفارة إنذار كي تتحرك.

في حين اختارت الإمارات أن تمزج بين الطموح والابتكار، فحوّلت الأمن السيبراني إلى رافعة استراتيجية للتحول الرقمي، ودمجته في كل مشروع وطني منذ لحظة التصميم، مستثمرة في مختبرات التهديدات وحاضنات الابتكار، لتجعل من القرار السيبراني أداة استباقية تُعيد تشكيل المستقبل قبل أن يفرضه الخطر.

وعلى اختلاف السياقات، تلتقي هذه النماذج عند حقيقة واحدة: أن السيادة الرقمية لم تعد تُقاس بالقدرة على الردّ على الهجمات فقط، بل بالقدرة على هندسة الوقاية، وبناء الثقة، وإعادة تعريف العلاقة بين الدولة والمواطن والمعلومة .فالقرار لم يعد مجرد خيار إداري يُمارس في الطوارئ، بل صار عقلًا جمعيًا يُبنى بالوعي، ويُترجم بالحوكمة، ويُشفَّر في الخوارزميات التي تدير الحياة اليومية.

وهكذا، تُغلق هذه التجارب صفحة الاستجابة التقليدية، وتفتح أفقًا جديدًا للسيادة الرقمية كـ بنية وجودية للدولة المعاصرة :بعضها يولد من صدمة، وبعضها من حكمة، وبعضها من حلم، لكنها جميعًا تؤكد أن مستقبل الدول لن يُحسم في ميادين القتال التقليدي، بل في قدرة أنظمتها على اتخاذ القرار السيبراني في صمت، قبل أن يصل الخطر إلى العلن.

### 6.6.5 تحليل فشل القرار في أحداث تسريب بيانات حساسة

البيانات في العصــر الرقمي باتت مرآة للهوية، وعنوان للثقة، وأحد أهم مظاهر السيادة الحديثة. ولهذا، فإن الطريقة التي تُدار بها حوادث تسريب البيانات تكشف أكثر مما يبدو على السطح؛ فهي تكشف جوهر القرار المؤسسي: هل يستند إلى الشفافية والمسؤولية؟ أم يتوارى خلف الخوف والمصالح التجارية؟ التجارب أثبتت أن الخطر الأكبر لا يكمن في الاختراق ذاته، بل في لحظة القرار، عندما تختار المؤسسة الصمت أو التأجيل بدلًا من المواجهة.

إحدى أبرز الأمثلة على ذلك ما حدث مع شركة Yahoo. ففي عام 2016، أعلنت الشركة عن اختراق تاريخي شمل بيانات أكثر من ثلاثة مليارات حساب مستخدم. غير أن الفضيحة لم تكن في حجم الاختراق وحده، بل في أن الحادثة وقعت قبل الإعلان بسنوات وظلت طيّ الكتمان بدافع حماية السمعة السوقية . القرار بالتأجيل قضى على الثقة مضاعفة، وأثبت أن الثغرة الأخطر لم تكن في الخوادم، بل في غرفة القرار.

أما Facebook، فقد واجهت أزمة مختلفة مع فضيحة Cambridge Analytica. لم يكن الأمر مجرد تسريب للبيانات، بل صمتٌ أوليّ استمر حتى انكشف أن ملايين الملفات الشخصية استُغلت لأغراض سياسية وتجارية. وكما صرّح المُبلّغ Christopher Wylie: "We exploited Facebook to harvest millions of people's profiles and target their inner demons" (The Guardian, 2018). وأكد تقرير البرلمان البريطاني أن الشركة "انتهكت عمدًا قوانين الخصوصية ومكافحة الاحتكار ."هنا، لم يكن الفشل في التقنية، بل في الأخلاق، حيث تغلّبت الحسابات السوقية على الشفافية.

وفي عام 2017، تعرضت Equifax لاختراق ضخم طال بيانات أكثر من 145 مليون مستخدم. لكن الشركة لم تُعلن عن الحادثة إلا بعد أسابيع، ما أثار غضبًا شعبيًا واسعًا. وخلص تقرير U.S. GAO (2018) إلى أن الشركة "أخفقت في تطبيق ممارسات أمنية أساسية وتأخرت في الإفصاح، مما قوّض ثقة الجمهور بشكل كبير". بذلك، تحوّل التأخير من وسيلة للسيطرة على الأزمة إلى دليل على غياب القرار السيادي.

أما Uber فقدّمت مثالًا أكثر فداحة. ففي 2016، تسرّبت بيانات حوالي 57 مليون مستخدم وسائق. وبدل الإعلان، دفعت الشركة 100 ألف دولار للمخترقين عبر ما سُمي Bug Bounty، مقابل التزامهم الصمت .(FTC, 2018) لم يُكشف عن الحادث إلا بعد عام، ما جعل القرار ليس مجرد خطأ إداري، بل انهيارًا أخلاقيًا عميقًا.

تُظهر هذه الأمثلة أن المشكلة ليست دائمًا في ضعف الأدوات أو الأنظمة التقنية، بل في هشاشة القرار نفسه. ففي اللحظة الحرجة، خضعت القرارات لمنطق العلاقات العامة والتسويق، بدل أن تُصاغ بمنطق السيادة والمسؤولية. ومن هنا يمكن القول إن "الأزمة الحقيقية ليست في الاختراق، بل في غياب النموذج الأخلاقي للقرار السيبراني."

فالقرار السيادي لا يُقاس بعدد الخوادم ولا بجدران الحماية، بل بقدرة المؤسسة على الاعتراف بالشجاعة، ومواجهة الخطر بشفافية، وبناء الثقة من جديد.

"في عالم السيادة الرقمية، لا يكفي أن تمنع الاختراق؛ بل يجب أن تمتلك الشجاعة الكاملة للاعتراف به، والاستعداد للمحاسبة عليه".

### 6.7 استخلاص الدروس وبناء إطار قرار سيادي متين

بعد استعراضنا للحالات المتنوعة – من أزمات كشفت هشاشة الأنظمة إلى تجارب صاغت مسارات سيادية جديدة – يتضح أن القرار السيبراني لم يعد مجرّد رد فعل على الخطر، بل أصبح بنية متكاملة من التفكير الاستراتيجي، والوعي المؤسسي، والمرتكزات الأخلاقية. القرار اليوم يُبنى مسبقًا، في فضاء تتداخل فيه السياسة بالاقتصاد، والتقنية بالقيم، ليصوغ إطارًا سياديًا قادرًا على مواجهة المجهول. ومن التجارب، يمكن استخلاص ستة أبعاد أساسية لبناء قرار سيبراني راسخ:

**1. القرار كتحصين استباقي لا كعلاج بعد الأزمة**

الهجمات التي لم تقع بعد هي الأخطر، لأنها تنتظر ثغرة في الخيال قبل أن تستغل فجوة في النظام. لذلك، لا تُقاس السيادة بقدرة الدولة على سرعة الرد فقط، بل بقدرتها على التخيل والتحضير لما وراء الأفق. إن ما نسميه "التخيل التحليلي" هو جوهر الوقاية: الجمع بين الحدس الاستراتيجي والتحليل العلمي لصياغة سيناريوهات تُهندس قبل وقوع الخطر. من لا يتخيل المستقبل، يفاجأ به. ومن لا يصمم احتمالاته، يصبح أسيرًا لها.

**2. القرار كفعل أخلاقي شفاف**

في عالم رقمي سريع، تصبح الشفافية خط الدفاع الأول. فحين تختار مؤسسة الصمت أو التأجيل، فهي لا تخسر بياناتها فقط، بل تخسر ثقة جمهورها. القرار السيبراني النزيه يعني الاعتراف، وتفسير الخطأ، وتحويل الفشل إلى درس. أما

التستر، فهو يضاعف الأزمة بدل أن يحلها. بذلك، تصبح الشفافية ليست مجرد قيمة أخلاقية، بل أداة استراتيجية لحماية السمعة، وترسيخ الثقة العامة.

### 3. القرار كمنظومة لا كفرد

القرار السيبراني الفعّال لا يُصاغ في لحظة إلهام فردي، بل في منظومة متكاملة تعمل كفريق واحد. من السياسات إلى التدريب، ومن الثقافة الأمنية إلى توزيع الأدوار، يجب أن يكون القرار ثمرة منظومة واعية، لا جهدًا بطوليًا فرديًا. السيادة هنا تعني أن تمتلك المؤسسة قدرة جماعية على الاستجابة، بحيث لا تنهار بسقوط حلقة، بل تصمد بفضل التنسيق والتكامل.

### 4. القرار المضمَّن في البرمجة

مع صعود الذكاء الاصطناعي، لم يعد القرار فعلًا يُتخذ في الاجتماعات فقط، بل صار يُكتب في الخوارزميات. من يُبرمج الأنظمة يحدد مسبقًا ما يُعتبر تهديدًا، وكيف يُستجاب له. وهذا يعني أن السيادة لا تقتصر على امتلاك البيانات، بل تشمل القدرة على فهم كيف تُصاغ القرارات داخل الأكواد. فالقرار المؤتمت ليس محايدًا، بل يعكس قيم ومصالح من كتب الشفرة. السيادة الرقمية الحقيقية هي أن نكون نحن من نكتب خيوط القرار، لا أن نُقاد بها دون وعي.

### 5. القرار كموقف فلسفي من الخطر

ليست كل الثغرات كارثة، بل قد تكون فرصة لإعادة البناء. هنا يظهر القرار السيادي كموقف: هل نرى في الانكشاف نهاية، أم بداية؟ هل نتعامل مع الفشل كوصمة، أم كدرس يعيد صياغة المنظومة؟ القرار ليس مجرد استجابة تقنية، بل

إعلان فلسفي: نحن لا ننكر الخطر، بل نواجهه ونتعلم منه. السيادة هنا هي القدرة على تحويل كل انكشاف إلى طاقة لإعادة البناء، بدلًا من أن يكون سببًا للإنكار.

**6. القرار كتجسيد لهوية المؤسسة الرقمية**

في النهاية، القرار السيبراني يعكس هوية المؤسسة نفسها: قيمها، أولوياتها، وصورتها أمام جمهورها. من نحن في الفضاء الرقمي؟ ما حدودنا السيادية؟ ما الذي نعتبره خطًا أحمر؟ هذه الأسئلة لا تُجاب في لحظة الأزمة، بل تُزرع في عمق الثقافة المؤسسية. القرار الذي ينبع من هوية واضحة هو قرار ثابت، يعلن عن ذات المؤسسة قبل أن يدافع عن أنظمتها.

إن السيادة الرقمية تمثل العقل العميق والقرار النزيه. هي قدرة على رؤية الخطر قبل أن يظهر، وعلى تحويل الأزمة إلى درس، وعلى جعل القرار مرآة للهوية والثقة. ومن دون هذه الأبعاد الستة، سيظل القرار السيبراني مجرّد رد فعل عابر. أما حين تتجذر هذه الأبعاد، يصبح القرار فعل سيادة متكاملًا، يثبت أن الحماية ليست في الأدوات وحدها، بل في وضوح البوصلة وصدق الاختيار.

## خاتمة الفصل

عند تأمل مسار الأمثلة والدروس المستخلصة، يتضح أن الأمن السيبراني للبنى التحتية الوطنية لم يعد مسألة تقنية صرفة، بل قضية وجودية تمس جوهر السيادة . فالهجمات التي استهدفت شبكات الكهرباء، والمياه، والطاقة، والاتصالات، لم تكتفِ بتعطيل الخدمات، بل كشفت قدرة خصوم غير مرئيين على التأثير في القرار السياسي، وتقويض الثقة العامة، وإرباك وظائف الدولة الأساسية. ومن ثم، فإن التحدي الحقيقي لم يعد في بناء أنظمة دفاعية تستجيب بعد وقوع الحادثة، بل في صياغة إطار سيادي استباقي يجعل الوقاية جزءًا من التصميم المؤسسي نفسه.

لقد أثبتت التجارب أن القرار السيبراني الرشيد يقوم على ثلاث مرتكزات رئيسة: أولًا، التحصين الاستباقي عبر تبني فلسفات مثل "انعدام الثقة" والدفاع متعدد الطبقات، بما يحوّل الخطر المتوقع إلى سيناريو مدروس. ثانيًا، الشفافية الأخلاقية التي تجعل من الاعتراف المبكر بالحوادث أداة لتعزيز الثقة المجتمعية لا تهديدًا لها. وثالثًا، المأسسة الجماعية للقرار، بحيث يُوزَّع عبء الحماية عبر منظومة متكاملة تشمل الأفراد والمؤسسات والتشريعات، بدل أن يُختزل في جهد فردي أو قطاعي محدود.

كما بيّنت النماذج الدولية أن اختلاف السياقات لا يلغي القاسم المشترك: ففي إستونيا وُلدت السيادة الرقمية من رحم الأزمة، وفي سنغافورة صيغت كمنهج وقائي مستمر، بينما في الإمارات جرى دمجها في مشروع التحول الرقمي الوطني كرافعة للابتكار. هذا التنوع يبرهن أن الأمن السيبراني لم يعد وظيفة دفاعية، بل عنصرًا مكوّنًا في تعريف الدولة الحديثة وصياغة هويتها.

إن خاتمة هذا الفصل يبرز حقيقة محورية :حماية البنى التحتية الوطنية ليست غاية تقنية، بل شرط وجودي لاستمرار الدولة في عصر رقمي تتداخل فيه الأكواد مع القرارات، والشبكات مع السيادة، والتهديدات مع وعي المجتمع .فالسيادة لم تَعُد تُقاس بقدرة الدولة على ردّ الهجوم بعد وقوعه، بل بقدرتها على تصميم مؤسساتها وهندسة قراراتها بحيث لا يتحول التهديد إلى أزمة، ولا الانكشاف إلى انهيار .وبهذا، يغدو الأمن السيبراني ليس فقط خط دفاع عن الدولة، بل إطارًا حضاريًا لبقائها واستقلال قرارها في عالم معقد متغير.

# الفصل السابع

# بناء منظومات قرار سيادية متكاملة

# مقدمة الفصل

إنّ جوهر السيادة في عصرنا الراهن لم يَعُد محصورًا في القدرة على الردّ الفعّال، بل في القدرة على **تخيّل الخطر قبل أن يتشكّل**، وهندسة بيئة القرار بحيث تكون صانعة للظروف لا رهينة لها. وهنا يتجلّى القرار السيبراني كمعمار حيّ، لا ينفصل فيه القائد عن المحلّل، ولا المعلومة عن الخوارزمية، ولا التشريع عن البنية التقنية. فالمعمار السيبراني يبدأ من غرف العمليات الوطنية، ويمتد إلى الشبكات المترابطة بين أجهزة الدولة ومنصات الذكاء الاصطناعي، ويعمل عبر مستويات متعددة من الاستشعار والتحليل والقيادة والتصميم الاستباقي.

وفي قلب هذا المعمار، يتقدّم التكامل بين الإنسان والآلة بوصفه ضرورة سيادية، لا خطرًا وجوديًا. فالآلة قادرة على السرعة والكفاءة، لكنها تفتقر إلى السياق والذاكرة الأخلاقية، في حين يوفّر الإنسان معيار الرحمة والبُعد القيمي. ومن هنا، تبرز الحاجة إلى إعادة صياغة العلاقة بين **التحليل البشري والقرار المؤتمت**، بحيث يُضبط عمل الأتمتة لا بمعايير الكفاءة التقنية فقط، بل بمعايير الوعي الوطني وحدود الأخلاق والسؤال السيادي الأعمق: من يقرّر؟ ولماذا؟

بهذا، تصبح غرف العمليات السيبرانية الوطنية أكثر من مراكز مراقبة؛ إنها **مصانع للقرار ومختبرات للتوقع** .ففيها لا تُرصد التهديدات فحسب، بل تُبنى السيناريوهات وتُترجم البيانات إلى بصيرة استراتيجية. ومع ذلك، يبقى الاختبار الحقيقي لهذه المنظومات في ميدان الفوضى والضباب والضغط، حيث يُقاس القرار بقدرته على الصمود تحت التشويش والتضارب لا في ظروف الاستقرار. وهنا يبرز دور التدريب

الحيّ والمحاكاة الواقعية في صناعة القرار السيبراني كفعل وجودي لا مجرد وظيفة إدارية.

إن السؤال المركزي الذي يطرحه هذا الفصل هو :**كيف يمكن للدولة أن تنتقل من إدارة الأزمات إلى إعادة صياغة شكل الأزمة نفسها؟** كيف تتحوّل السياسات من ردود أفعال إلى أفعال سيادية من مستوى أعلى، تُعيد ترتيب الزمن وتكتب سيناريو الأحداث قبل أن يُفرض عليها؟ وكيف تنتقل من دولة تمتلك مؤسسات تقنية، إلى دولة تُهندس وعيها السيبراني في الخفاء، داخل بروتوكولات الاتصال، وأكواد الدفاع، وخطط الإغاثة الرقمية؟

لقد بات واضحًا أن الدول التي لا تملك منظومة قرار سيادي متكاملة، ستجد نفسها في لحظة الأزمة رهينة لقرارات صاغها الآخرون داخل خوارزميات لا تسيطر عليها، وشبكات لا تديرها، وبرمجيات تُراقبها أكثر مما تُراقبها هي. وعليه، فإن **القرار السيبراني أصبح اليوم ليس مجرد وسيلة تنظيم، بل ساحة صراع، وأداة قوة، وعلامة وجود للدولة الحديثة.**

من هنا ينطلق هذا الفصل السابع ليتناول **هندسة القرار السيبراني**، باعتبارها المستوى الأعلى الذي تتقاطع فيه التقنية مع الفلسفة، والسياسة مع الذكاء الاصطناعي، والسيادة مع الخوارزمية. وهي تسعى للإجابة عن السؤال المصيري: كيف تُبنى قرارات المستقبل في فضاءٍ لم يَعُد يعترف بالزمن التقليدي، ولا يمنح الدول ترف الانتظار؟

### 7.1 القرار السيادي كمنظومة متكاملة

إن جوهر هذا المعمار يقوم على مبدأ التكامل: فلا يكفي أن تمتلك الدولة أدوات تقنية متقدمة دون إطار قانوني يحكمها، ولا يجدي التشريع وحده دون إرادة سياسية توجهه، ولا تنجح الإرادة السياسية ما لم تتجذر في وعي مجتمعي قادر على حماية ذاته. بهذا، يصبح القرار السيادي شبكة متداخلة، لا يُختزل في عنصر واحد، بل يتوزع عبر منظومة شاملة.

1. **المستوى السياسي: صياغة الرؤية والسيادة العليا**

في هذا المستوى تُرسم الخطوط العريضة لمفهوم السيادة وأولويات الأمن القومي. القرارات السياسية تحدد ما هي الأصول السيادية الحرجة، وما هي حدود المصلحة الوطنية في الفضاء السيبراني. فالدول التي تبنت استراتيجيات وطنية للأمن السيبراني – مثل إستونيا أو الولايات المتحدة – وضعت الأمن الرقمي في صلب استراتيجياتها الأمنية، معتبرة أن أي اختراق لمنشأة طاقة أو شبكة مالية يوازي تهديدًا مباشرًا للسيادة.

السياسة هنا ليست مجرد قرارات فوقية، بل هي هندسة توجهات تُترجم إلى قوانين واستثمارات وتوزيع للموارد. وبغياب هذا المستوى، تتحول القرارات التقنية إلى ردود أفعال معزولة، بلا بوصلة استراتيجية.

2. **المستوى القانوني: ترسيخ الشرعية وصياغة الأطر**

القانون هو الأداة التي تمنح القرار طابعه المؤسسي والملزم. في الاتحاد الأوروبي مثلًا، مثّل النظام العام لحماية البيانات GDPR إطارًا تأسيسيًا أعاد تعريف العلاقة بين الدولة والمواطن والشركات الرقمية. هذا التشريع لم يقتصر على حماية

الخصوصية، بل أصبح أداة سيادية تمكّن الدول من فرض شروطها على شركات عابرة للحدود مثل Google و.Facebook

إطار القانون في السياق السيبراني لا يُقنن فقط الحقوق الرقمية، بل يضع قواعد للمحاسبة، والإفصاح، والتعاون الدولي .إنه الدرع الذي يحمي من الانفلات، والمرساة التي تثبّت القرار السيادي في بيئة متسارعة يصعب ضبطها.

**3. المستوى التقني: العقل التنفيذي ومنظومة الذكاء**

في هذا المستوى يُترجم القرار السياسي والقانوني إلى أنظمة تقنية قادرة على العمل في الزمن الحقيقي .هنا نجد أنظمة الاستشعار المبكر، منصات الذكاء الاصطناعي التي تحلل البيانات، ومراكز العمليات السيبرانية التي تُراقب وتستجيب للهجمات لحظة وقوعها.

لكن البعد الأهم هو أن التقنية لم تعد مجرد أدوات، بل أصبحت فاعلًا سياديًا بحد ذاتها. فالخوارزميات التي تكتبها الدولة تعكس فلسفتها في التعامل مع الخطر: هل تعتمد على "الثقة المسبقة"، أم على "التحقق المستمر"؟ هل تصمم نظمها بحيث ترد بعد الهجوم، أم بحيث تمنعه من الأساس؟ إن ما يُبرمج في الأكواد هو قرار سياسي مقنّن بلغة تقنية.

**4. المستوى المجتمعي: المواطن كشريك سيادي**

لا يمكن لأي قرار سيادي أن يصمد إذا ظل محصورًا في غرف العمليات أو مكاتب المسؤولين. إن الفضاء السيبراني هو فضاء جماعي، والمواطن فيه ليس مستخدمًا فقط، بل هدفًا وخط دفاع في آن واحد.

التجارب الدولية أوضحت أن بناء وعي مجتمعي يُمثل سلاحًا غير تقليدي .ففي سنغافورة، مثلًا، يُدرّس الأمن السيبراني في المدارس، ويُدمج في الثقافة اليومية، بحيث يصبح المواطن شريكًا في حماية وطنه .(Chong, 2020) وفي إستونيا، تُعتبر الهوية الرقمية جزءًا من العقد الاجتماعي، مما يُحوّل المواطن إلى عنصر فعّال في معادلة الأمن الوطني.

**التكامل بين المستويات الأربعة**

**إن ما يميز هذه المنظومة هو التناغم البنيوي بين عناصرها:**

- **السياسة تُحدد الاتجاه.**
- **القانون يضبط الإطار.**
- **التقنية تُنفّذ وتستشعر.**
- **المجتمع يشارك ويحصّن.**

أي خلل في مستوى من هذه المستويات يفتح ثغرة تُهدد المنظومة بأكملها. فإذا امتلكت الدولة أدوات تقنية متقدمة بلا وعي مجتمعي، ستظل عرضة لهجمات الهندسة الاجتماعية. وإذا امتلكت قوانين صارمة بلا قدرات تقنية، ستتحول النصوص إلى حبر على ورق. وإذا وجدت الإرادة السياسية بلا تشريعات واضحة، ستبقى القرارات معلّقة بلا أدوات تنفيذية.

**السيادة كشبكة لا كمركزية مطلقة**

إن صمود الدولة السيبرانية لا يُبنى على المركزية، بل على التوزيع: أي أن تُصمم المنظومة بحيث يُعوّض قصور عنصر بقوة عنصر آخر. بهذا يصبح القرار السيادي

شبكة معقدة، لا تنهار إذا تعطلت نقطة، بل تستمر بفضل مرونة توزيع الأدوار. إنها هندسة resilience لا هندسة.control

## 7.2 أبعاد بناء منظومة القرار السيادي

إن بناء منظومة قرار سيادي في المجال السيبراني يعد عملية حضارية متكاملة، تُعيد صياغة العلاقة بين الدولة، المواطن، والمعلومة. القرار هنا ليس فعلًا لحظيًا، بل بنية عقلية وسياسية وقانونية وتقنية تمتد من الخوارزمية إلى التشريع، ومن وعي الفرد إلى فلسفة الدولة. ومن خلال تحليل التجارب الحديثة، يمكن تمييز ستة أبعاد أساسية تمثّل الأعمدة الكبرى التي يقوم عليها القرار السيبراني الرشيد.

### 7.2.1 البعد الاستباقي (الوقاية والتخيّل التحليلي)

إن أخطر التهديدات ليست تلك التي نراها اليوم، بل تلك التي تتشكل في صمت، وتنتظر لحظة غفلة لتتحوّل إلى أزمة. لذلك فإن جوهر السيادة لا يقوم على سرعة الرد فقط، بل على القدرة على التخيّل التحليلي :(Analytical Imagination) أي الجمع بين التحليل العلمي للبيانات والحدس الاستراتيجي لرسم سيناريوهات مستقبلية.

يتضح أن الدول التي اعتمدت مقاربة استباقية نجحت في بناء مرونة سيبرانية (Cyber Resilience)تقلل من وقع الهجمات قبل أن تتحول إلى كوارث وطنية. هذه القدرة على "رؤية ما وراء الأفق" هي ما يجعل الدولة قادرة على التحكم بزمن الأزمة، فلا تُفاجأ، بل تكون مستعدة بما يكفي لتوجيه الحدث بدل أن تُقاد به.

### 7.2.2 البعد الأخلاقي (الشفافية والمسؤولية)

الأمن السيبراني لا يُقاس فقط بما تملكه المؤسسات من جدران نارية أو تقنيات ذكية، بل يتجلى أيضًا في **القرار الأخلاقي لحظة الخطر** .فحين تختار مؤسسة إخفاء ثغرة أو الصمت عن حادثة حمايةً لسمعتها، فإنها تزرع بذور فقدان الثقة، وهي بذور قد تنمو إلى أزمة مستمرة لسنوات.

لقد أثبتت **فضيحة** Yahoo **عام 2016** أن الضرر الأكبر لم يكن في عملية الاختراق ذاتها، بل في قرار التأجيل الذي قوّض مصداقية الشركة على مستوى عالمي .وبالمثل، كشفت **قضية** Cambridge Analytica أن صمت Facebook الأولي لم يكن مجرد خطأ إداري، بل انحرافًا عن مبدأ الشفافية، الذي يُعد أساسًا للأمن والثقة معًا.

من هنا، تُصبح **الشفافية ليست مجرد قيمة أخلاقية، بل أداة استراتيجية** :فهي التي تعزز الثقة العامة، وتُضعف الشائعات، وتُبقي العلاقة بين الدولة ومواطنيها قائمة على الصدق والمساءلة، أي على ما هو أثمن من البيانات ذاتها .

### 7.2.3 البعد المؤسسي (القرار كمنظومة لا كفرد)

القرار السيبراني الناجح لا يُصاغ في مكتب مغلق ولا في لحظة إلهام فردي. إنه ثمرة منظومة مؤسسية متكاملة تعمل بتنسيق محكم بين المستويات السياسية، القانونية، التقنية، والمجتمعية. كما يشير(2014) Singer & Friedman ، فإن "السيادة الرقمية ليست فعلًا تقنيًا، بل ممارسة جماعية تتوزع عبر البنية الوطنية."

فحين يكون القرار موزعًا ومؤسسيًا:

- يُصبح التدريب الدوري جزءًا من السيادة،
- ويُحوَّل كل موظف إلى عنصر في شبكة الدفاع،
- وتُبنى آليات اســتجابة لا تعتمد على بطل فردي، بل على قدرة جماعية للصمود.

هذا التكامل المؤسسي هو ما يجعل الدولة قادرة على امتصاص الصدمات دون أن تنهار بنيتها، لأن الســيادة حينها لا تكون محصــورة في رأس الهرم، بل ممتدة عبر كل طبقاته.

### 7.2.4 البعد التقني (القرار المبرمج والمؤتمت)

لقد انتقل القرار في العصــر الرقمي من طاولة الاجتماعات إلى ســطر الكود . فالخوارزميات اليوم لا تُنفّذ القرار فقط، بل تُعيد تعريفه مســبقًا: من يكتب الكود يحدد معايير التهديد، وآليات الاستجابة، وأولويات التدخل.

لكن الخطر يكمن في أن هذه الخوارزميات ليست محايدة؛ فهي تحمل بصمة من صمموها، وتتحكم عمليًا في مسارات القرار دون أن يعي صانع السياسة حجم هذا التأثير. لذلك، فإن الســيادة الرقمية تتطلب أن تمتلك الدولة كودها الســيادي، وأن تفرض ضــوابط قانونية وأخلاقية على أنظمة الأتمتة، حتى لا تتحوّل الخوارزميات إلى "سلطة غير مرئية" تُدار من الخارج.

### 7.2.5 البعد الفلسفي (موقف من الخطر والتهديد)

الهجوم السيبراني ليس مجرد خلل تقني؛ إنه سؤال وجودي .المؤسسات التي ترى في الانكشاف مرآة للتعلم تُحوّل التهديد إلى فرصة، بينما المؤسسات التي تنكر أو تُخفي تفقد القدرة على إعادة البناء.

وهكذا يصبح القرار إعلانًا فلسفيًا بقدر ما هو خطة عملية:

- هل نرى في الثغرة نهاية أم بداية جديدة؟
- هل نقرأ الفشل كوصمة، أم كدرس تأسيسي؟

هذه القدرة على تحويل الأزمة إلى منصة للنمو هي ما يجعل القرار السيادي أكثر من مجرد استجابة تقنية؛ إنه إعلان عن فلسفة الدولة في مواجهة المجهول.

### 7.2.6. البعد الهوياتي (القرار كتعبير عن الذات السيادية)

في النهاية، لا ينفصل القرار عن هوية الدولة. فالقرار السيبراني يُجسد القيم الوطنية والحدود الحمراء، ويعكس تعريف الدولة لذاتها في فضاء رقمي لا يعترف بالحدود التقليدية.

إن سؤال "من نحن في الفضاء السيبراني؟" لم يعد سؤالًا فلسفيًا مجردًا، بل أصبح أساس كل قرار:

- هل نُعرّف أنفسنا كدولة منتجة للمعرفة أم مستهلكة لها؟
- هل نمتلك أدواتنا، أم نُقاد بأدوات الآخرين؟
- هل قراراتنا نابعة من داخلنا، أم مفروضة علينا من الخارج؟

القرار هنا ليس مجرد حماية للبنية التحتية، بل إعلان متكرر عن هوية الدولة وحدود سيادتها الرقمية.

إن هذه الأبعاد الستة تتشابك لتُشكل "معمار القرار السيادي". فالبعد الاستباقي يحصّن المستقبل، والبعد الأخلاقي يحمي الثقة، والبعد المؤسسي يضمن الصمود الجماعي، والبعد التقني يصوغ القرار في الخوارزميات، والبعد الفلسفي يمنح الرؤية، والبعد الهوياتي يحدد المعنى.

وبذلك، يصبح القرار السيبراني ممارسة سيادية متكاملة، تتجاوز فكرة "الحماية الأمنية" إلى "هندسة حضارية" تُعيد تعريف الدولة في زمن تُدار فيه القوة والسيادة عبر الأكواد بقدر ما تُدار عبر الجيوش.

## 7.3 . أدوات بناء منظومات القرار السيادي

يتطلب بناء منظومة القرار السيادي أدوات عملية قادرة على ترجمة هذه المبادئ إلى واقع تشغيلي. فالأمن السيبراني لم يعد مجرد خطط مكتوبة أو سياسات معلنة، بل منظومة معقدة من الأدوات المؤسسية والتقنية التي تعمل بتناغم لتشكيل عقل وطني قادر على الاستباق، الاستجابة، والتكيّف مع المتغيرات. ويمكن تلخيص أبرز هذه الأدوات في أربع ركائز رئيسة:

### 7.3.1 غرف العمليات السيبرانية الوطنية – مصانع القرار

تمثل غرف العمليات السيبرانية (National Cyber Operations Centers) قلب المنظومة السيادية في زمن المعلومات. فهي ليست مجرد مراكز مراقبة للشبكات أو أنظمة إنذار مبكر، بل مصانع للقرار حيث تتحوّل البيانات الخام إلى بصيرة قابلة للتنفيذ.

إن هذه الغرف تؤدي وظائف استراتيجية:

- الرصد اللحظي (Real-time Monitoring): مراقبة تدفقات البيانات وتحديد الأنماط غير المألوفة.
- التحليل المتكامل (Integrated Analysis): ربط الأحداث التقنية بالسياقات السياسية والاقتصادية.
- إدارة الأزمات (Crisis Management): تحويل الإشارات الرقمية إلى قرارات عملياتية وسياسية.

بهذا، تصبح غرفة العمليات جهازًا عصبيًا وطنيًا، يُعيد إنتاج السيادة في الزمن الرقمي عبر قراءة سريعة للتهديدات وترجمتها إلى خيارات عملية تحفظ استقرار الدولة.

### 7.3.2 مختبرات التهديدات وحاضنات الابتكار (Cyber Ranges)

في ظل تسارع التهديدات، لم يعد كافيًا أن تملك الدولة خططًا مكتوبة على الورق. بل لا بد من مختبرات تدريبية حية تُحاكي الهجمات في بيئات افتراضية واقعية، تُعرف باسم Cyber Ranges.

تُعد هذه المختبرات حاضنات للابتكار الأمني، حيث يتم:

- تدريب الكوادر على مواجهة سيناريوهات هجومية متطورة.
- اختبار أنظمة الدفاع في بيئات مشابهة للواقع.
- تطوير حلول جديدة عبر التجريب المستمر.

دولة الإمارات العربية مثلًا استثمرت في إنشاء حاضنات تهديدات تُستخدم لتدريب المؤسسات الوطنية على سيناريوهات هجومية معقدة، مما عزز قدرتها على الاستباق بدل الاكتفاء بالرد . وهكذا تتحوّل هذه المختبرات إلى مدارس سيادية لإنتاج عقل أمني يقظ، قادر على التعامل مع المجهول وكأنه حدث يومي متوقع.

### 7.3.3 الأطر المرجعية الدولية(NIST, ISO/IEC, EU NIS2)

لا يمكن للقرار السيادي أن يُبنى في فراغ؛ فهو يحتاج إلى **أطر مرجعية معترف بها عالميًا** تُرسي قواعد التصميم والتشغيل، وتمنح القرارات المشروعية والاتساق. ومن أبرز هذه الأطر:

- **إطار** NIST **للأمن السيبراني**:(NIST Cybersecurity Framework) يُعد من أكثر المراجع استخدامًا عالميًا، إذ يوفّر خارطة عمل مرنة لتقييم المخاطر، وتحديد الثغرات، وبناء الضوابط الأمنية الملائمة بما يتناسب مع طبيعة كل مؤسسة أو دولة.(NIST, 2018)
- **المعيار الدولي**:ISO/IEC 27001 يُرسّخ قواعد إدارة أمن المعلومات ضمن نظام إداري متكامل، يربط بين السياسات والإجراءات والضوابط الفنية، ويُطبَّق على مستوى المنظمات والدول بوصفه معيارًا للثقة والاعتماد الدولي.(ISO/IEC, 2013)
- **التوجيه الأوروبي**:NIS2 يُمثل نقلة تشريعية مهمة في الاتحاد الأوروبي، إذ يفرض التزامات صريحة على القطاعات الحيوية لضمان مستوى عالٍ من الأمن السيبراني، ويعزز منسوب التنسيق العابر للحدود في مواجهة الهجمات المتزايدة.(European Commission, 2022)

تكمن أهمية هذه الأطر في أنها تجعل الأمن جزءًا من التصميم منذ البداية (Security by Design)، بدل أن يُلحق لاحقًا كإجراء وقائي. وبذلك، تصبح البنية التحتية الوطنية أكثر صلابة، وتتحول القوانين والمعايير إلى "دستور خفي" ينظم فضاء السيادة الرقمية.

### 7.3.4 التكامل بين الإنسان والآلة

لقد أصبح القرار السيبراني اليوم نتاجًا لتفاعل مستمر بين العقل البشري والخوارزمية. فالأنظمة الذكية القائمة على الذكاء الاصطناعي قادرة على تحليل ملايين الإشارات في لحظات، لكنّها تفتقر إلى البوصلة الأخلاقية والسياق السياسي. وهنا يأتي دور الإنسان كمُشرف وصاحب قرار نهائي.

وكما يشير(2020) Rid ، فإن أخطر ما قد تواجهه الدولة ليس الهجوم ذاته، بل فقدان القدرة على إدراك من يسيطر على القرار: هل هو الإنسان، أم الكود، أم مزيج غير متوازن بينهما؟

لذلك، فإن بناء منظومة سيادية متكاملة يقتضي وضع أطر حوكمة للأتمتة تضمن أن تظل الخوارزميات خادمة للقرار الوطني، لا صانعة له بشكل مستقل. إن التوازن بين سرعة الآلة وحكمة الإنسان هو ما يجعل القرار السيادي متينًا وقادرًا على مواجهة التهديدات دون أن يفقد بعده الأخلاقي أو السياسي.

تشكل هذه الأدوات الأربع – غرف العمليات، مختبرات التهديدات، الأطر المرجعية، والتكامل الإنساني–الآلي – البنية التحتية الخفية للقرار السيادي .فمن خلالها، تتحول البيانات إلى بصيرة، والأزمات إلى فرص تدريب، والقوانين إلى شبكات حماية، والخوارزميات إلى أدوات مُسخّرة للسيادة.

إن الدولة التي تمتلك هذه الأدوات وتدمجها في نسيجها المؤسسي لا تُدافع عن سيادتها فقط، بل تُعيد صياغة مفهومها في عصر تُخاض فيه المعارك عبر الأكواد بقدر ما تُخاض عبر الجيوش.

### 7.4 التحديات في بناء منظومات القرار

الهندسة السيبرانية للقرار تعمل في بيئة عالية التعقيد، حيث تتقاطع السرعة التكنولوجية مع بطء التشريع، ويصطدم مبدأ السيادة بواقع الاعتماد الخارجي، ويُضاف إلى ذلك هشاشة البُنى البشرية والثقافية في مواجهة التهديدات الداخلية، فضلًا عن المعضلة الأخلاقية بين الإفصاح والسرية. هذه التحديات ليست ثانوية، بل هي التي تُحدد مدى قدرة الدولة على الانتقال من ردّ الفعل إلى الفعل السيادي المتكامل.

#### 7.4.1 التعقيد التشريعي

يُعد البُعد القانوني من أعقد التحديات، إذ تسعى الدول إلى صياغة قوانين وتشريعات تُواكب التسارع التقني. بطبيعة الحال، يتحرك التشريع وفق إيقاع بطيء يقتضي مشاورات برلمانية ومجتمعية مطوّلة، بينما تتغير البيئة الرقمية بوتيرة شبه يومية. هذا التفاوت يخلق فجوات قانونية تسمح بظهور مناطق رمادية غير مُغطاة، تُستغل من قبل الفاعلين السيبرانيين أو حتى من قبل الشركات الكبرى.

على سبيل المثال، ما تزال العديد من الدول النامية والمتقدمة على السواء تحاول تكييف تشريعاتها مع متطلبات **اللائحة الأوروبية**NIS2 ، التي تُلزم البنى التحتية الحيوية بمعايير صارمة للأمن السيبراني وإدارة المخاطر. التحدي هنا مزدوج: كيف

تُسرّع الدولة من إنتاج التشريعات دون التضحية بجودتها وشرعيتها السياسية، وكيف تُحوّل النص القانوني إلى ممارسة قابلة للتطبيق داخل المؤسسات التقنية؟

### 7.4.2 الاعتماد الخارجي

التبعية التقنية ليست مجرد مسألة اقتصادية، بل هي خطر استراتيجي على السيادة ذاتها. فالدولة التي تعتمد بشكل مفرط على أنظمة تشغيل، أو منصات سحابية، أو برمجيات أجنبية قد تجد قرارها مرهونًا لإرادة مزوّد خارجي، أو لضغوط جيوسياسية.

يشير Nye (2022) إلى هذا الواقع بمصطلح **"التبعية الرقمية"**، حيث تصبح بعض الدول "مستهلكة للتكنولوجيا" بدلًا من كونها صانعة لها، مما يجعلها أكثر هشاشة أمام أي قيود أو نزاعات تجارية.

وتزداد خطورة هذا التحدي مع توسع الاعتماد على خدمات السحابة العالمية (Cloud Services) والذكاء الاصطناعي المُدار من قبل شركات كبرى. ففي حال تم تعليق الخدمة أو التحكم في البيانات، فإن القرار الوطني نفسه قد يتأثر بشكل مباشر. من هنا، يصبح بناء القدرات المحلية وتطوير الصناعة التقنية الوطنية عنصرًا جوهريًا لتقليل الاعتماد الخارجي وتعزيز الاستقلال السيادي.

### 7.4.3 التهديدات الداخلية

رغم أن الخطاب العام يركّز غالبًا على التهديدات الخارجية، إلا أن الدراسات الحديثة تُظهر أن الخطر الداخلي لا يقل أهمية. تُشير تقارير IBM (2022) إلى أن أكثر من 40٪ من الحوادث السيبرانية تنبع من الداخل، سواء نتيجة الإهمال غير المقصود، أو ضعف التدريب، أو الاستغلال الخبيث من قبل موظفين ذوي

صـلاحيات عالية. الموظف الذي يضـغط على رابط تصـيّد (Phishing) أو يسـيء استخدام امتيازاته قد يشكل تهديدًا يفوق قدرة أي جدار ناري على الحماية.

الحل هنا لا يكمن فقط في الأدوات التقنية، بل في بناء **ثقافة أمنية مؤسـسـية** تجعل كل موظف جزءًا من خط الدفاع الأول. التدريب المسـتمر، توزيع الصـلاحيات، وإرسـاء ثقافة المسـاءلة، كلها آليات تُمكّن المؤسـسـات من تحويل الفرد من نقطة ضعف إلى عنصر صمود. فالأمن السيبراني، في جوهره، لا يقوم على التقنية فقط، بل على الوعي البشري الذي يُديرها.

### 7.4.4 توازن الشفافية والسرية

يُعد هذا البُعد من أعقد معضـلات القرار السـيادي: كيف يمكن تحقيق التوازن بين الإفصـاح الذي يُعزز ثقة الجمهور، والسـرية التي تحمي الأمن الوطني؟ الإفراط في الشـفافية قد يمنح الخصـوم معلومات حسـاسـة حول طبيعة الدفاعات والثغرات، بينما يُفضي التكتّم المفرط إلى فقدان الثقة الشعبية وتفشي الشائعات.

التاريخ الحديث مليء بالأمثلة، ومنها ما أظهرته تقارير (2018) FTCعن شـركة Uber، التي أخفت اختراقًا ضـخمًا لبيانات 57 مليون مسـتخدم خوفًا من فقدان سـمعتها السـوقية، لكنها خسـرت الثقة العامة بشـكل مضـاعف حين انكشـف الأمر لاحقًا. في المقابل، تُظهر بعض التجارب أن الاعتراف السريع والمسؤول – حتى مع إبراز الثغرات – قد يُحافظ على ثقة الجمهور ويدعم صورة المؤسسة ككيان مسؤول.

من هنا، تصبح السيادة الرقمية اختبارًا للقدرة على صياغة **سياسة اتصالية رشيدة** : تُفصح بقدر ما يحمي الثقة العامة، وتكتم بقدر ما يحفظ أمن الدولة.

إن التحديات في بناء منظومات القرار السيادي لا تكشف فقط عن ضعف في التقنية أو فجوات في التشريع، بل تكشف عن سؤال وجودي أعمق: هل تستطيع الدولة أن تُدير الخطر بوصفه بيئة دائمة، لا مجرد حالة طارئة؟ إن التحدي الأكبر ليس في سدّ كل ثغرة، بل في بناء **مرونة سيادية** (Resilience) قادرة على امتصاص الصدمات، والتكيّف مع التحولات، وتحويل الأزمات إلى فرص لإعادة هندسة المنظومة الوطنية.

## 7.5 نموذج FAIR (Factor Analysis of Information Risk)

يُعتبر نموذج FAIR (Factor Analysis of Information Risk) من أكثر الأطر التحليلية نضجًا وتطورًا في مجال تقييم المخاطر المعلوماتية والسيبرانية. ما يميّزه عن غيره من النماذج التقليدية أنه ينقل النقاش من مستوى "المخاطر المرتفعة أو المنخفضة" ذات الطابع الانفعالي والانطباعي إلى أفق التحليل الكمي القابل للقياس والمقارنة. في النسخة السيادية، لا يقف FAIR عند حدود دعم المؤسسات التقنية، بل يتجاوزها إلى ربط الخطر بالمصالح الوطنية، وتحويل الغموض إلى قرار، والتقديرات إلى معمار معرفي يبنى عليه صانع القرار السيادي خياراته الإستراتيجية.

### 7.5.1 الحاجة إلى FAIR في السياق السيادي

غالبًا ما تُعرض المخاطر في المؤسسات أو الأجهزة الحكومية بلغة فضفاضة، مثل: "الخطر مرتفع" أو "الوضع حرج". هذه المصطلحات، وإن بدت مألوفة، لا تساعد على تحديد الأولويات أو المفاضلة بين بدائل الاستجابة. هنا يظهر FAIR كإطار فكري وتحليلي يفرض قاعدة معرفية بسيطة: **لا يمكن اتخاذ قرار رشيد في مواجهة الخطر دون القدرة على قياسه** —even **بشكل تقريبي**. هذه القاعدة تغيّر شكل

النقاش، حيث يعاد ترتيب المخاطر وفق احتمالية حدوثها وكلفتها المتوقعة، بدلًا من الضجيج الإعلامي أو ضغط اللحظة. وقد أكدت الأطر المرجعية الحديثة مثل NIST Cybersecurity Framework 2.0على ضرورة تبني مقاربات كمية في تقييم المخاطر لتعزيز الحوكمة وتوجيه الموارد.

### 7.5.2 البنية الأساسية للنموذج

يقوم FAIR على مقاربة ثنائية الأبعاد :**معدل وقوع الحدث الخاسر** (Loss Event Frequency – LEF)و **حجم الخسارة**.(Loss Magnitude)

- البعد الأول (LEF) يُشتق من عنصرين رئيسيين :**تكرار محاولات التهديد** (Threat Event Frequency – TEF)، و**قابلية الاختراق** (Vulnerability) التي تحدد احتمالية نجاح تلك المحاولات.
- أما البعد الثاني (Magnitude) فيتضمن **الخسائر الأولية** (مثل توقف الأنظمة أو الخسائر المالية المباشرة)، و**الخسائر الثانوية** )مثل فقدان السمعة، التداعيات القانونية، أو الأثر السياسي.(

وتُدمج هذه العناصر في معادلة بسيطة لكنها قوية:

**الخطر الكلي = معدل التكرار × حجم الخسارة**

هذه الصياغة تحول الخطر من شبح غامض إلى قيمة كمية قابلة للمقارنة، ما يمكّن متخذ القرار من ترتيب الأولويات، وتوزيع الموارد بوعي، وموازنة تكلفة الوقاية مع تكلفة الإهمال.

### 7.5.3 ما الذي يجعل FAIR مختلفًا؟

يمتاز FAIR بعدة سمات تجعله مختلفًا عن الأطر الأخرى:

1. **التقدير المنضبط** :لا يشترط دقة مطلقة، بل يتيح نطاقات تقديرية Range) (Estimatesتعكس حقيقة اللايقين في البيانات.
2. **محاكاة** :Monte Carlo يستخدم طرقًا رياضية لمحاكاة آلاف السيناريوهات المحتملة، ما يوفّر توزيعًا احتماليًا للخطر بدل رقم واحد جامد.
3. **ثقافة الحساب لا الخوف** :يغيّر FAIR الثقافة المؤسسية من الانفعال إلى الحساب، إذ تُبنى القرارات على المقارنة الكمية لا على الانطباعات.
4. **قابلية التكامل** :يمكن دمج FAIR مع أطر مثل ) NISTIR 8286الذي يربط الأمن بإدارة المخاطر المؤسسية (ERM ومع ISO/IEC 27005الخاصة بإدارة المخاطر الأمنية.

### 7.5.4 FAIR كأداة سيادية لصناعة القرار

في المستوى السيادي، يُصبح FAIR أكثر من مجرد أداة تقنية، بل إطارًا لبناء **اقتصاد قرار وطني** .فهو يمكّن الدولة من:

- **بناء خرائط مخاطر قطاعية** تربط بين الطاقة، الصحة، المال، النقل والاتصالات، مع إعطاء وزن احتمالي وكلفي لكل تهديد.
- **تبرير الاستثمارات الأمنية** بلغة كمية مفهومة على المستويين الوزاري والتشريعي، ما يعزز الشفافية والمساءلة.

- **صـــياغة خطاب عام قائم على الأدلة** بدل خطاب التخويف، بما يرفع ثقة المواطنين والشركاء الدوليين.
- **اســـتباق التهديدات** عبر نمذجة ســـيناريوهات متعددة، وتوجيه الموارد إلى المخاطر ذات الوزن الحقيقي الأعلى.

هذا التوجه يتماشـــى مع التحولات العالمية نحو ربط القرارات الأمنية بإدارة المخاطر المؤســـسية(ERM) ، كما ورد في توصـيات NISTIR 8286 وCSF 2.0 (NIST, 2020; NIST, 2024).

### 7.5.5 تحديات التطبيق

رغم قوة النموذج، تواجه المؤسسات والدول عدة تحديات في تبنيه:

- **نقص البيانات التاريخية الدقيقة** التي تغذي النماذج الكمية.
- **ضـعف الثقافة المؤسـســية التحليلية،** حيث ما زال الكثيرون يعتمدون على الحدس بدلاً من الحساب.
- **مقاومة التغيير على المســتوى القيادي،** إذ قد يعتبر بعض القادة أن التحليل الكمي يهدد سلطتهم المبنية على الخبرة الشخصية أو الحدس.
- **صعوبة دمج النتائج الكمية في السياسات** دون وجود بنية تشريعية داعمة.

إن التحولات الرقمية المتســارعة والتعقيد المتنامي للهجمات الســيبرانية يجعلان الحاجة إلى إطار FAIR أكثر إلحاحًا من أي وقت مضـــى. فبدل أن تبقى الدول رهينة قرارات تقوم على التخمين أو ردود الفعل الإعلامية، يقدّم FAIR قدرة منهجية على تحويل الخوف إلى حساب، والضبابية إلى نطاقات مقيسة، والتهديدات

إلى فرص لإعادة البناء .وكما تؤكد أدبيات FAIR الحديثة :المعرفة لا الخوف هي أول أدوات السيادة .

يمثل FAIR نقلة نوعية في التفكير بالمخاطر؛ فهو ليس مجرد أداة تقنية، بل بنية فكرية وسيادية تعيد صياغة عملية صناعة القرار في زمن اللايقين. ومن خلال دمجه مع الأطر الدولية الحديثة مثل NIST CSF 2.0 وNISTIR 8286 وISO/IEC 27005، يتحول FAIR إلى أداة استراتيجية تمكّن المؤسسات والدول من صياغة قرارات رشيدة، قائمة على الحساب الكمي لا الانطباع، وقادرة على الاستباق الفعّال بدل الاكتفاء بالرد اللاحق.

إن جوهر القيمة في FAIR يكمن في قدرته على إعادة تعريف المخاطر كلغة مشتركة بين صانع القرار والمسؤول الفني والجهة التنظيمية، حيث تتلاقى الرؤية السيادية مع الحساب العلمي، لتشكّل أساسًا لحوكمة متينة واستجابة تتجاوز الدفاع إلى البناء.

على سبيل المثال، يُظهر تطبيق FAIRفي أحد البنوك الوطنية كيف يمكن تحويل التهديدات المعقدة إلى حسابات كمية واضحة: فبدل الاكتفاء بتقديرات عامة حول "خطر الاختراق"، استخدم البنك نموذج FAIR لقياس الاحتمال السنوي للخسارة المالية الناتجة عن هجوم فدية، وربطه بمؤشرات تشغيلية مثل *زمن الكشف* (MTTD)و*زمن الاستجابة*(MTTR) ؛ الأمر الذي مكّن الإدارة من تخصيص ميزانية دقيقة لتعزيز أنظمة النسخ الاحتياطي وتدريب الموظفين، وإقناع مجلس الإدارة والجهات التنظيمية بأن الاستثمار في الأمن لم يعد تكلفة غامضة بل قرارًا اقتصاديًا محسوبًا، يحقق حماية سيادية للبنية التحتية المالية ويُرسّخ الثقة المجتمعية.

## 7.6 قيادة القرار السيبراني في أوقات الأزمات الوطنية

في الأزمات السيبرانية الحادّة، يُصبح التحرّك السريع المبني على تقدير احتمالي منضبط شرطًا حاسمًا للحد من الأثر التقني والاجتماعي، وللاحتفاظ بزمام السرد العام. وتُظهر التجارب المستقاة من تمارين محاكاة واسعة النطاق مثل Cyber Stormو Locked Shieldsأنّ الدقائق الأولى تحدّد عمق الاختراق ومن يمتلك رواية الحدث .(CCDCOE, 2023)كما تؤكد توجيهات وزارة الأمن الداخلي الأمريكية أنّ التسمية المبكرة والصادقة لطبيعة الهجوم جزء من الدفاع السيادي ذاته .(DHS, 2020)ويحذّر تحليل الوكالة الأوروبية للأمن السيبراني (ENISA) من أنّ التردّد يخلّف "فراغًا سرديًا" يملؤه الخصم لتوجيه الرأي العام .(ENISA, 2022)

إجمالًا: في الهجوم السيبراني الحاد، كل دقيقة تعني مساحة اختراق إضافية وكلفة استعادة أعلى .لذلك، لا تنتظر القيادة "الصورة الكاملة" قبل التحرك؛ بل تبادر بقرارات سريعة ومحسوبة، تسمّي ما يجري بوضوح منذ البداية، وتُحافظ على التحكم في الرواية العامة، مانعةً تضليل المجتمع أو شلّ ثقة الجمهور.

**ما المقصود بالتقدير الاحتمالي المنضبط؟**

- استخدام نطاقات تقديرية بدلًا من رقمٍ قطعي واحد.
- وضع عتبات فعل جاهزة (Action Thresholds)بحيث يُفعّل القرار عند تخطيها تلقائيًا.
- اتخاذ قرار أولي سريع، مع حفظ الأدلة وإجراء التحليل الجنائي دون تعطيل الاستجابة.

- تحديث القرار دوريًا مع تدفّق الأدلة.

إنها معادلة توازن بين سرعة العزل والاحتواء من جهة، ودقّة التواصل العام المتدرج من جهة أخرى، دون إفراط في الكشف أو تهوين يُضعف الثقة.

**الساعة الأولى هي لحظة الحسم**

خلال الساعة الأولى من الهجوم، تُبنى معادلة النجاة:

- تفعيل قيادة موحّدة ذات صلاحية قرار واضحة.
- تصنيف الحادث رسميًا وإعلان نطاقه المبدئي.
- عزل الأجزاء المصابة وخفض الخدمة بطريقة آمنة مع إبقاء بدائل تشغيلية.
- حفظ السجلات الرقمية دون مسح أو إعادة تهيئة.
- إصدار بيان مبكر يوضح: ما نعرفه، ما لا نعرفه، وما الذي يجري فعله.
- إشعار الجهات المنظمة والشركاء عبر قنوات آمنة.
- قياس الأثر عبر مؤشرات مثلMTTD/MTTR ، تدهور الأداء، ومستوى ثقة الجمهور.

**أربع زلات قاتلة يجب تفاديها**

1. انتظار الوضوح التام قبل التصرف.
2. تنفيذ إيقاف شامل غير ضروري يُضرّ بالمجتمع.
3. إطلاق رسائل متضاربة بين الجهات الرسمية.

4. اعتماد تواصل عام إمّا مفرط يكشف أكثر مما ينبغي أو مُهوّن يفقد الثقة.

**مؤشرات المسار الصحيح**

نحن على الطريق السليم عندما نلحظ:

- احتواءً ناجحًا يمنع تمدد الهجوم أفقيًا.
- استعادة تدريجية للخدمات مع الحفاظ على الأدلة.
- رسالة حكومية موحّدة تُقلّص الشائعات وتُثبت الرواية الرسمية.
- تحسنًا ملحوظًا في مؤشري الكشف والاستجابة عبر التحديثات المتتابعة.

**المعادلة الذهبية**

عند اكتمال الحدث، يُختصر جوهر الحماية السيادية في معادلة واحدة:

**سرعة محسوبة + تسمية مبكرة صادقة + اتصال موحّد قائم على تقدير احتمالي متجدّد = حماية مزدوجة للسيادة: تقنيًا (تقليل الأثر) وسرديًا (امتلاك الرواية).**

### 6.7.1 طبيعة القرار السيبراني وقت الأزمة

في لحظة الانكشاف السيبراني، تتحرّك الفيزياء المؤسسية بسرعةٍ مختلفة: الزمن ينضغط، والمعلومة تأتي ناقصة، والمسؤولية تتشابك، والقرار يكتسب معنى رمزيًا يتجاوز التقنية. ما يلي يشرح هذه الأبعاد الأربعة بأسلوب سردي–علمي، ويُسنِدها إلى أدبيات وتمارين ميدانية موثوقة.

**أولًا: الزمن المضغوط**

الدقائق الأولى تختصر «تاريخ الأزمة» كله. فبُنى الهجوم الحديثة وسلاسل القتل (Kill Chain) تَزيد أثرها مع كل دقيقة تأخير، ما يرفع مساحة الاختراق وكلفة الاستعادة (MTTR) ويصعّب احتواء الانتشار الأفقي داخل الشبكات. دروس تمارين Locked Shields و Cyber Storm تُظهر أن القرار المبكر لا يحصر الضرر فحسب، بل يحسم أيضًا من يعرّف الحدث للداخل والخارج؛ التأخر يسلّم «حق التسمية» للخصم ويضاعف التعافي اللوجستي والاقتصادي لاحقًا (CCDCOE, 2023). ولهذا تؤكد إرشادات الاستجابة الوطنية أن «تسمية ما يجري مبكرًا وبصدق» جزء من الدفاع نفسه، لا ملحقٌ اتصاليّ به.

**ثانيًا: المعلومة الناقصة**

في الساعات الأولى، الإشارات متضاربة: هل هو اختراق فعلي أم إنذار كاذب؟ فعل خارجي أم خطأ داخلي؟ الانتظار حتى اكتمال الصورة يعني قرارًا سلبيًا يمنح الخصم زمام المبادرة. البديل العلمي هو «التقدير الاحتمالي المنضبط»: قرارات أولية مبنية على نطاقات تقدير وعتبات فعلٍ مُحدَّدة سلفًا، تتحدث دوريًا مع تدفّق الأدلة الجنائية الرقمية (rolling updates). هذا ما توصي به أدلة الحوكمة الاتصالية أثناء الحوادث: قل ما تعرفه وما لا تعرفه وما الذي ستفعله تاليًا، ثم حدّث التقدير كلما تحسّنت الرؤية.

**ثالثًا: المسؤولية المركّبة**

القرار وقت الأزمة ليس «زرّ عزلٍ تقني». إنه حزمة سيادية متزامنة: حماية الخدمات الحيوية واستمرارية الأعمال، ضبط الخطاب العام ومنع الفراغ السردي، تنسيق عابر للمؤسسات (صحة/ طاقة/ مال/ داخلية)، وتفعيل التزامات تنظيمية

وقانونية وربما إجراءات سياسية طارئة. تقارير WannaCry في منظومة NHS أظهرت أن غياب التنسيق والاختبار المسبق لخطط الاستجابة ضاعف الارتباك رغم بساطة بعض الإجراءات التقنية المطلوبة. وكذلك كشفت أزمة Colonial Pipeline أن القرارات الاتصالية والاقتصادية (كإعلان الحادث ودفع الفدية واستردادها لاحقًا) جزءٌ من «هندسة السيادة» بقدر ما هي إجراءات تقنية.

**رابعًا: الرمزية السيادية**

تُقاس القرارات بقدرتها على إثبات حضور الدولة بوصفها «الفاعل المُقرِّر»، لا بمجرد نجاحٍ تقني معزول. السيطرة المبكرة على توصيف الحدث تغلق نافذة «الفراغ السردي» التي يستغلها الخصم للتضليل وإرباك الجمهور، بينما الرسائل المتضاربة تُقوّض الشرعية وتُطيل أمد الأزمة الاجتماعية حتى لو انحلّت تقنيًا .لذا تشدّد أدبيات التمارين العملياتية على أن القيادة التي تنتظر وضوح الصورة تكون عمليًا قد فقدت حقّ الفعل؛ والسيادة هنا تُستعاد بقرارٍ واضح وفي توقيتٍ صحيح.

في الأزمات الحادّة :سرعةٌ محسوبة تحسم الكلفة، وتقديرٌ احتمالي متجدد يعوّض نقص المعلومات، وتنسيقٌ سيادي متعدد الأبعاد يمنع التفكك المؤسسي، ورسالة موحّدة مبكرة تصون الشرعية وتغلق الباب أمام السرد المعادي. هذه الأربعة معًا هي خط الدفاع الأول عن السيادة التقنية والسيادة السردية.

## 7.6.2 حالات دالّة من أزمات كبرى

### 1. NotPetya أوكرانيا 2017

ضرب «نوت بيتيا» كبَّادٍ (wiper) متنكّر في هيئة فدية، فشلَّ طبقاتٍ كاملة من الدولة: من محطات الطاقة والمرافئ وشبكات النقل إلى المصارف ووسائل

الإعلام. هنا لم يكن السؤال: "كيف نُصلِّح الخوادم؟" بل: "كيف تُواصل الدولة العمل وهي رقمياً خارج الخدمة؟". القرارات الحاسمة تمحورت حول تشغيل بدائل يدوية حرجة، وإعادة بناء الشبكات من نسخٍ نظيفة مع تجزئة صارمة، وتوحيد الرسالة العامة لمنع «فراغٍ سردي» يستثمره الخصم. الدرس المركزي: استمرارية الدولة وضبطُ الرواية أولًا، والإصلاح التقني يأتي ضمن هذا الإطار.

**.2** WannaCry **وقطاع الصحة البريطاني** 2017

أوقف «واناكراي» أجهزة وخدمات طبية وأجّل عملياتٍ جراحية، فصار القرار السيبراني قرارًا صحيًا–اجتماعيًا بامتياز. أظهر التحقيق أن قصور تفعيل خطط الاستجابة والقيادة الموحدة عمّق الارتباك المؤسسي وولّد صدمةً مجتمعية تمس الثقة في مؤسسة وطنية الرمز. العبرة: لا يكفي التصحيح التقني (ترقيعات/ عزل)، بل يلزم إطار قيادة عملياتي واتصالي يحمي استمرارية الرعاية، ويقول للناس ماذا يحدث وما الذي سيفعلونه الآن.

**.3** Colonial Pipeline **2021**

أدّى هجوم فدية إلى وقف إمدادات الوقود أيامًا وإثارة ذعرٍ جماهيري. الاستجابة لم تُقَم على إزالة البرمجية الخبيثة فقط، بل على حزمة سيادية: إعلانٌ مبكرٌ وشفاف يوازن ما يُقال وما لا يُكشف، تنسيقٌ فيدرالي سريع، وحسمٌ في المفاضلة بين استمرار الخدمة واحتواء المخاطر. لاحقًا أُعلن استرداد جزءٍ من الفدية، ما أعاد جزءًا من هيبة الرد العام ورسّخ السرد الرسمي أمام الجمهور.

هذه الوقائع تؤكد أن معيار النجاح في الأزمات السيبرانية يتخطّى مؤشراتٍ تقنية مثل زمن التعافي(MTTR) :

- استعادة السرد الوطني سريعًا تغلق نافذة التضليل وتمنع خصخصة الحقيقة.
- حماية الثقة العامة عبر اتصالاتٍ مبكرة صادقة ومتسقة بين الجهات.
- ضمان استمرارية الخدمات الحيوية حتى تحت انقطاعٍ رقمي، ببدائلٍ مدروسة ومفاضلاتٍ مُعلنة.

ان القرار الرشيد وقت الأزمة هو ثلاثيّ الأبعاد (تقنيٌ محسوب، واتصاليٌ موحّد، وسياديٌ يضمن الاستمرارية) به تُصان الدولة كفاعلٍ مقرِّر، لا كضحية حدثٍ تقني عابر.

### 7.6.3 من يملك القرار؟

في لحظة الهجوم السيبراني لا يكفي "العمل الجيد"، بل يلزم من يملك حقّ القرار وكيف يُمارَس هذا الحق بسرعة وبشكلٍ مُتَّسِق. لذلك تُبنى الجاهزية السيادية على بروتوكولٍ مُسبَق يحدّد بدقّة:

- **مركز القرار السياسي** :الرئيس/ مجلس الأمن الوطني لتحديد الحالة السيادية، إعلان الطوارئ، واعتماد المفاضلات الكبرى (تعطيل خدمة/ استمراريتها، طلب دعم دولي...).
- **السلطة الفنية التنفيذية** :الهيئة الوطنية للأمن السيبراني/ غرفة العمليات الوطنية لإدارة الحادث لحظيًا (العزل، التجزئة، التحليل الجنائي، استعادة الخدمة).

- **أدوار القطاعات المتأثرة** :الطاقة، المال، الصحة... بما يشمل صلاحيات كل قطاع وواجباته في الإبلاغ والاحتواء واستمرارية الأعمال.

لماذا هذا التفصيل مهم؟ لأن غموض الصلاحيات في اللحظة الحرجة يولِّد فراغًا سياديًا :تتباين القرارات، تتضارب الرسائل، فيملؤه الخصم بالرواية المضادّة والإعلام بالتكهنات والجمهور بالذُعر. هنا تُوصي أدلة ENISA الحديثة بأن تُحدَّد سلاسل التفويض، ومسارات التصعيد، وواجهات الاتصال الموحدة قبل وقوع الأزمة، وأن تُمارَس في تمارين دورية. وبالمنطق نفسه، تؤكد نسخة NIST CSF 2.0 أن "الحوكمة الفعّالة" تستلزم وضوح الأدوار والمسؤوليات ومتطلبات الإبلاغ واتخاذ القرار عبر المؤسسة والدولة.(NIST, 2024)

**ما هي «هندسة القرار متعددة المستويات» عمليًا؟**

هي إطار يعمل من **غرفة عمليات وطنية موحَّدة** ذات ولاية قانونية واضحة، ويجمع أربعة مسارات متوازية ومتكاملة:

1. **المسار السياسي–السيادي** :يقرر عتبة إعلان الحادث كطوارئ وطنية، يُجيز إجراءات استثنائية (مثل تفعيل الشبكات الاحتياطية أو الاستعانة بالدعم الدولي).
2. **المسار الأمني–التنسيقي** :يضمن مواءمة الجهات الأمنية والاستخباراتية، وإدارة الاعتمادية بين القطاعات (تأثير حادث في الاتصالات على المال/ الصحة...).
3. **المسار الفني–العملياتي** :يقود العزل المرحلي، التجزئة، الحفاظ على الأدلة، وخطط الاستعادة؛ ويُصدر "أوامر تقنية مُلزِمة" لمشغلي البنى الحرجة.

4. **المســار الاتصــالي–العام** :يوفّر **صــوتًا واحدًا** للدولة: ماذا نعرف/ لا نعرف؟ ماذا نفعل الآن؟ ما المطلوب من الجمهور والقطاع الخاص؟ مع ضــبط ما يُكشــف حفاظًا على الأمن العملياتي.

**عناصر التشغيل التي تمنحك السرعة والمشروعية**

لا يكتمل بناء الجاهزية الســيبرانية دون توافر عناصــر تشــغيلية واضــحة، تمنح عملية اتخاذ القرار كلًّا من **الســرعة** في الاســتجابة و**المشــروعية** في التنفيذ. ويمكن تلخيص هذه العناصر في خمس مرتكزات رئيسية:

1. **التفويض المُســبق**:(Pre-delegation) يتمثل في وثيقة قانونية مُعتمدة تُحدّد بدقة الجهة المخوّلة بالتصــرف عند تخطي مســتويات خطر مُعرّفة ســلفًا .(Action Thresholds)هذا التفويض يمنع التردد ويضمن سرعة الاستجابة في اللحظات الحرجة.

2. **مصــفوفة المســؤوليات**:(RACI Matrix) أداة تنظيمية تُوزّع الأدوار وفق منطق "المســؤول – المعتمِد – المســتشــار – المُخطَر"، بحيث تكون كل جهة على دراية بمهامها في القرارات المتكررة، مثل عزل قطاع، أو خفض خدمة، أو إرسال إشعار للجهات المنظمة.

3. **مركز قيادة موحّد**:(Unified Command) غرفة عمليات مشــتركة تضــم ضــباط ارتباط من كل قطاع معني، بما يقلل من زمن اتخاذ القرار، ويعزز التنسيق الأفقي بين المؤسسات، ويمنع الازدواجية أو تضارب الإجراءات.

4. **قواعد الاتصال**:(Communication Protocols) تعتمد على تعيين متحدث رسمي واحد، مدعوم برسائل قياسية مُعدّة سلفًا تتضمن: ما هو معروف، وما هو مجهول، والخطوات التالية .(What / Unknown / Next Steps) يهدف ذلك إلى ملء الفراغ السردي ومنع الشائعات أو تضارب الخطاب .

5. **مقاييس الحُكم**:(Governance Metrics) مؤشرات كمية تُستخدم لتقييم الأداء، مثل تقليص زمن كمون القرار(Decision Latency) ، وضمان اتساق الرسائل بين الجهات، ومراقبة مؤشرات الاكتشاف والاستجابة (MTTD/MTTR)عبر تحديثات دورية .

**ماذا يحدث إن غاب هذا الإطار؟**

- قرارات متعارضة (وزارة تُغلق ومنظمٌ يمنع الإغلاق)،
- فقدان السيطرة على الرواية،
- إهدار للأدلة الرقمية،
- وتأخير يضاعف عمق الاختراق وكلفة الاستعادة.

باختصار :غياب الوضوح يُبطئ التقنية ويقوّض الشرعية

وهكذا فان بروتوكولٌ مُسبَق، وصلاحياتٌ مُعرَّفة قانونيًا، وقيادةٌ موحَّدة متعددة المستويات من غرفة عمليات وطنية—هذه هي وصفة الجمع بين السرعة والمشروعية ووحدة السرد في الأزمات السيبرانية، كما توصي ENISA وتُطابقها مبادئ الحوكمة فيNIST CSF 2.0 .

### 7.6.4 القيادة وسط الفوضى

**أولًا: قيادة الاتصال.**

في الساعات الأولى من أي أزمة سيبرانية، يصبح كل بيان رسمي "فعلًا سياديًا". المطلوب خطابٌ مبكر يشرح باختصار: ما الذي نعرفه الآن، ما الذي لا نعرفه بعد، وما الذي نفعله ولماذا. هذه "الشفافية الذكية" تقلّص فراغ الشائعات وتحافظ على الثقة العامة دون تهويلٍ يثير الذعر أو تهوينٍ يضعف الجدية. ويُفضَّل توحيد الرسائل عبر متحدث واحد أو غرفة عمليات وطنية، مع تحديثات دورية قصيرة. هذا النهج توصي به تقارير ENISA لأنه يقطع الطريق على السرد المعادي ويثبت مصداقية الدولة.

**ثانيًا: قيادة المفاضلات.**

القرار في قلب العاصفة ليس تقنيًا فقط؛ إنه مفاضلة أخلاقية–سيادية بين ثلاث أولويات تتزاحم تحت ضغط الوقت: استمرارية الخدمة، وسلامة البيانات والأدلة الجنائية، وسمعة المؤسسة/ الدولة. لضبط هذه المفاضلة عمليًا: تُستخدم "تقديرات نطاقية" لاحتمالات الخطر، وعتبات فعل مُعرَّفة مسبقًا (مثل إيقافٍ مرحلي عند تجاوز مؤشّر اختراق معيّن)، مع توثيق سبب كل قرار وتأثيره المتوقع على المواطن والاقتصاد.

**ثالثًا: قيادة التنسيق المتقاطع.**

لا تُدار الأزمات الكبرى من قطاعٍ واحد. لذا تُفعَّل هندسة قرار متعددة المستويات (سياسي–أمني–فني–اتصالي) عبر مركز قيادة مدمج بصلاحيات واضحة. هذا المركز يطلق مسارات "استدعاء متبادل" بين الدفاع والطاقة والمال

والقطاع الخاص والدبلوماسية، ويشغّل بدائل تشغيلية مثل: العزل المرحلي للشبكات، الخفض الآمن للخدمة، التحويل إلى شبكات احتياط أو قنوات يدوية حرجة. الهدف: احتواء الأثر أفقيًا مع إبقاء الخدمات الأساسية في حدّها الأدنى الآمن.

**رابعًا: خصال القرار الرشيد في الأزمة.**

- وضوح :أوامر ولغة غير ملتبسة.
- سرعة حكيمة :تحرّك مبكر محسوب، لا اندفاعًا عشوائيًا.
- شجاعة سياسية :الاستعداد لقرارات مكلفة آنيًا (كإيقاف خدمة حرجة) لمنع ضرر أكبر.
- اتساق مؤسسي :رسالة واحدة وقناة قيادة واحدة.
- رمزية سيادية :يُظهِر القرار أن الدولة هي الفاعل المُقرِّر، لا الحدث أو الخصم.

في الفوضى، تقود الدولة بثلاثة خيوط متزامنة—اتصال موحّد يثبت الثقة، مفاضلات أخلاقية–عملية تحت عدم اليقين، وتنسيق متقاطع سريع—وبذلك تحمي السيادة التقنية والسردية معًا.

### 7.6.5 الاستشراف كسياسة ما قبل الأزمة

الاستباق السيادي معناه أن نبني منظومة القرار قبل أن تقع الأزمة. عمليًا، نعامل "الزمن قبل الهجوم" كمساحة عمل منهجية: نلتقط مؤشرات مبكرة، نُصمّم سيناريوهات محتملة، نُحاكي تفاعلات القطاعات، ثم نحوّل كل ذلك إلى قواعد

قرار واضحة. هذا يتوافق مع دورات **التعرّف–الوقاية–الكشف–الاستجابة–التعافي** في إطار NIST المحدث، ومع منهجية **تقدير/ معالجة/ مراقبة المخاطر** في ISO/IEC 27005، بحيث لا تكون الجاهزية وثيقة على الرف، بل مسارًا حيًّا يُراجع دوريًا.

**أول لبنة هي تحليل الإشارات الضعيفة**

مؤشرات صغيرة ومتفرّقة—ارتفاع غير مألوف في حركة خدمة حسّاسة، تغيّر في سلوك برمجية مفتوحة المصدر، أو نمط تصيّد جديد—تسبق الأحداث الكبيرة. نجمع هذه الإشارات من مصادر متعددة، نمنحها درجات ملاءمة ومصداقية، ونبحث عن ترابطها عبر الزمن. الهدف ليس إنتاج إنذار قاطع، بل إنذار "له وزن" يطلق فعلًا احترازيًا محسوبًا عندما تتجاوز المؤشرات عتبة متفقًا عليها.

**بعدها ننتقل إلى بناء السيناريوهات المركّبة**

المستقبل ليس خطًا واحدًا؛ نصوغ عدة مسارات "معقولة" وفق محاور عدم اليقين (هوية الخصم، الأثر، زمن التصعيد، القطاع المتأثر)، ونربط كل سيناريو بخيارات استجابة وموارد مطلوبة. ولأن الواقع شبكة تفاعلات، نكمّل ذلك بـ نماذج محاكاة ديناميكية تُظهر التأثيرات المتسلسلة: كيف ينعكس تعطيلٌ في قطاع الطاقة على سلاسل التوريد، والقطاع المالي، والرأي العام؟ عبر هذه المحاكاة نفهم أين نُجزّئ الشبكات، ومتى نلجأ لخفضٍ آمن للخدمة، وكيف نعيد التوازن دون كلفة اجتماعية مفرطة.

**وبالتوازي، نُعدّ خرائط اتجاهات**

تُترجم التحولات الكبرى (كالذكاء الاصطناعي، والتشفير، والتشريعات العابرة للحدود) إلى نقاط قرار عملية. نُقيّم أثر كل اتجاه على الأصول الحرجة

والالتزامات النظامية، ونُدخل النتائج في سجل المخاطر المؤسسي. بذلك نحافظ على بوصلة إستراتيجية محدثة بدل سياسات تتقادم سريعًا مع تغيّر البيئة التقنية والتنظيمية.

**قواعد الاشتباك الزمنية**

ولكي تتحوّل هذه الأدوات إلى فعل، نصوغها على هيئة قواعد اشتباك زمنية بسيطة ومُلزِمة :*إذا* ظهر المؤشر X بحدةٍ تتجاوز العتبة المتفق عليها، *نفعّل* القرار Y )تجزئة فورية، خفضٌ آمن للخدمة، تشغيل قنوات بديلة، وبيان أولي موحّد خلال دقائق(، *لتفادي* النتيجة Z (انتشار أفقي للهجوم أو فقدان السرد العام). تُكتب القواعد بتقديرات نطاقية لا أرقام يقينية، وتُراجع تكراريًا عبر حلقة خطّط–نفّذ–تحقّق–حسّن، وبمشاركة متعددة التخصصات تضم السياسة والقانون والتقنية والاقتصاد والأخلاق.

وأخيرًا، نقيس أننا على الطريق الصحيح بمؤشرات بسيطة لكنها كاشفة: انخفاض زمن الكشف والاستجابة(MTTD/MTTR) ، تحسّن دقة الإنذار المبكر، اتساع تغطية السيناريوهات الحرجة في التمارين، وثبات الثقة المؤسسية والجماهيرية أثناء الاختبارات أو الحوادث الفعلية. بهذه السلسلة المترابطة—من الإشارة الضعيفة إلى القاعدة الزمنية—نبني سيادة تُسبق الحدث وتقلّص هوامش مفاجآت الخصوم.

### 7.6.6 التحديات البنيوية للاستشراف والجاهزية

تتعثر القدرة الاستباقية للمؤسسات عندما تُدار بمنطق "إطفاء الحرائق" بدلاً من منطق بناء المرونة. ويعود ذلك غالبًا إلى هيمنة الحوافز قصيرة الأمد ودورات الميزانيات الضاغطة نحو نتائج فورية، مما يهمّش الاستثمار في التمارين، والمحاكاة،

وتنمية القدرات طويلة المدى. وتكمن المعالجة في حوكمة مستندة إلى الأدلة، تربط التمويل ومؤشرات الأداء بنتائج التمارين الوطنية الدورية، مثل اختبارات الاختراق، والمحاكاة القطاعية، وتمارين مراكز العمليات. هذا الربط يضمن مكافأة الجهات التي تُظهر تحسنًا قابلاً للقياس في قدراتها على الكشف المبكر والاستجابة.

وتتعمق المشكلة أكثر مع اتساع فجوة الثقافة الاحتمالية لدى صُنّاع القرار، إذ يميلون إلى إسقاط نماذج خطية على بيئة شبكية معقدة. ويُعالج هذا القصور عبر إدخال ما يمكن تسميته بـ "التقدير المنضبط" في إجراءات العمل: استخدام نطاقات تقديرية بدلاً من الاكتفاء برقم واحد، تحديد عتبات فعل واضحة، وتشغيل محاكاة مبسطة) مثل (Monte Carlo ضمن خطط إدارة المخاطر. وتُستكمل هذه الإجراءات ببرامج تدريب قيادية قصيرة تُزوّد المسؤولين غير التقنيين بمهارة قراءة المخاطر كاحتمالات مرجَّحة، لا كيقين أو نفي قطعي.

أما سيطرة الطوارئ اليومية فتبتلع وقت التخطيط وتؤجل الاستثمار في مختبرات المحاكاة وفرق التحليل الاستباقي. ولتجاوز ذلك، يصبح من الضروري اعتماد آليات مؤسسية تضمن "زمنًا محميًا" للاستشراف يُدرج ضمن التقويم الحكومي، مع ميزانيات مُسوَّرة (ring-fenced) مخصصة لمراكز التدريب السيبراني cyber) (rangesوفرق التحليل التنبئي. كما أن نشر نتائج التمارين على مستوى مجلس الأمن الوطني يرسّخ التعلم المؤسسي، ويحوله إلى التزام تمويلي وتنفيذي حقيقي.

## خاتمة الفصل

يبين هذا الفصل أنّ السيادة الرقمية ليست ردّ فعلٍ على الخطر، بل هندسة قرار تُبنى قبل وقوعه، وتُدار أثناءه، وتُراجع بعده. جوهرها ثلاثيةٌ مترابطة: عقلٌ استباقي يلتقط الإشارات الضعيفة ويحوّلها إلى قواعد اشتباك زمنية؛ وحوكمةٌ متعددة المستويات تُحدّد بدقّة من يملك القرار وكيف يُمارسه؛ ومنهجٌ تشغيليّ في الأزمات يقوم على تقديرٍ احتماليّ منضبط يوازن بين سرعة الفعل ودقّة البيان. بهذه الثلاثية تنتقل الدولة من إدارة الأضرار إلى تصميم المسار.

اكد الفصل أنّ التكامل بين الإنسان والآلة ليس خيارًا تقنيًا بل ضرورة سيادية : الخوارزميات تُسرّع الرصد والتحليل، والإنسان يُضيف المعنى والشرعية الأخلاقية. يترجم هذا التكامل في غرف عمليات وطنية موحّدة، ومختبرات محاكاة Cyber) (Ranges، وأطر مرجعية معيارية (NIST/ISO/NIS2) تُحوّل الأمن إلى «تصميم منذ البداية» لا «ملحق علاجي». وفي قلب المنهج الكمي، يوفّر نموذج FAIRلغة مشتركة لتقييم المخاطر وتبرير المفاضلات الاستثمارية والسياسية بلغة أرقام قابلة للمقارنة.

وخلال الأزمات الحادّة، تختصر «الساعة الأولى» تاريخ الأزمة كله: تُثبّت خلالها الرواية الرسمية، وتُفعّل خطط العزل المرحلي والتشغيل البديل، وتبدأ تحقيقاتٌ فنية–قانونية تحفظ الدليل وتُغذّي قرارات محدثة بالتتابع. معيار النجاح لا يُقاس بالمؤشرات التقنية وحدها (MTTD/MTTR) بل بقدرة الدولة على استمرارية الخدمات وحماية الثقة وامتلاك السرد العام. هنا تظهر خصال القرار الرشيد: وضوحٌ

في اللغة، سرعةٌ حكيمة، شجاعةٌ سياسية، اتساقٌ مؤسسي، ورمزيةٌ تُثبت حضور الدولة كفاعل مُقرِّر.

وفيما قبل الأزمة، تُواجه منظومة الجاهزية تحدياتٍ بنيوية—ثقافة إطفاء الحرائق، ضعف التفكير الاحتمالي، وطغيان الطوارئ على التخطيط—لكن علاجها ممكنٌ عبر حوكمة دلائلية تربط التمويل بنتائج التمارين، وتعليمٍ احتماليّ للقادة، وزمنٍ محميّ للاستشراف. هكذا تُصبح «الإشارة الضعيفة» نقطة انطلاق لسلسلة تعلم–فعل–مراجعة تُقلّص مفاجآت الخصوم وتوسّع هامش مناورة الدولة.

وهكذا فان السيادة الرقمية تُصنع حين تجتمع الرؤية مع الأداة، والمعيار مع السلوك، والسرعة مع الانضباط. طريق التنفيذ واضح: تبنّي FAIR كلغةٍ للمخاطر، ترسيخ قيادةٍ موحّدة بصلاحيات مُسبقة، تشغيل مختبرات محاكاة وتمارين دورية، وصياغة قواعد اشتباك زمنية تُحدِّد «ماذا نفعل ومتى ولماذا». بهذا المعمار، لا تكتفي الدولة بحماية نفسها؛ بل تُعيد تعريف القوة في عصرٍ تُكتب فيه السيادة بالكود بقدر ما تُكتب بالقانون.

# الفصل الثامن

# السيادة الرقمية بين التحول العالمي والتجربة الأردنية

# من التحديات الكونية إلى النماذج الوطنية

# مقدمة الفصل

تُعَدّ السيادة الرقمية اليوم أحد أبرز مرتكزات القوة الوطنية في القرن الحادي والعشرين. إذ لم تعد القوة تُقاس فقط بامتلاك الموارد الطبيعية أو العسكرية، بل بمدى القدرة على إدارة البيانات، حماية البنية التحتية الرقمية، وصناعة القرار السيبراني .وفي ظل تزايد التهديدات العابرة للحدود، أصبحت الدول مطالبة بصياغة نماذج وطنية للسيادة الرقمية تعكس خصوصيتها الثقافية والسياسية، وتتكامل في الوقت ذاته مع المنظومة العالمية.

لقد فرض هذا التحول نفسه عبر تحديات عابرة للحدود .فقد كشفت الهجمات السيبرانية الكبرى – مثل Stuxnetالذي أصاب أنظمة نووية حساسة، و Industroyerالذي عطّل شبكات طاقة – أنّ الحرب قد تتحول إلى بضعة أسطر من الشيفرات القادرة على شلّ دول بأكملها. كما انتقلت المنافسة بين القوى العظمى من الأسواق التقليدية إلى السيطرة على البنى التحتية الرقمية والمنصات المعلوماتية العملاقة، فأصبح النفوذ الدولي يُقاس بقدرة الدول على التحكم في تدفق المعلومات ورسم قواعد الاقتصاد السيبراني.

وإلى جانب ذلك، فتح الذكاء الاصطناعي التوليدي الباب أمام إشكاليات غير مسبوقة حول طبيعة القرار ذاته: من يملك الكلمة الفصل حين تنتج الخوارزميات المعرفة والتوصيات؟ وكيف يمكن ضمان الشفافية والعدالة في قرارات تُصاغ آليًا قبل أن تمر بفلترة سياسية أو اجتماعية؟

أمام هذه التحولات، تقف الدول بين خيارين حاسمين: إما البقاء في موقع التبعية والاستهلاك، أو صياغة نماذج وطنية للسيادة الرقمية تُمكّنها من اتخاذ قرارات مستقلة تنبع من واقعها وتستجيب لخصوصياتها الثقافية والسياسية.

في هذا السياق، يبرز الأردن بوصفه مثالًا مهمًا؛ فموقعه الجغرافي، وتنوعه الاجتماعي، ورأسماله البشري الشاب تمنحه فرصة ليكون نموذجًا إقليميًا للسيادة الرقمية .الخطوات التي أُنجزت حتى الآن – مثل تأسيس المركز الوطني للأمن السيبراني، وسنّ التشريعات الخاصة بالجرائم الإلكترونية، وتطوير البرامج الأكاديمية – تمثل أساسًا متينًا، لكنه يحتاج إلى استكمال عبر خارطة طريق عملية تحوّل السيادة الرقمية من إطار نظري إلى منظومة قرار قابلة للتنفيذ.

ومن هنا، يأتي هذا الفصل ليقدّم قراءة مزدوجة: فهو من جهة يتناول التحولات العالمية التي تعيد تشكيل مفهوم السيادة، ومن جهة أخرى يعرض التجربة الأردنية بوصفها مختبراً لبناء نموذج وطني قابل للتطوير. كما يقترح خطة تنفيذية لبناء منظومة قرار سيادي خلال 90 يومًا، تنقل الدولة من منطق الاستجابة إلى منطق المبادرة وصناعة القرار الاستباقي.

بهذا، لا يُختتم الكتاب بعرض نظري، بل بطرح عملي متكامل يؤكد أن السيادة الرقمية هي جوهر السيادة الوطنية في العصر الحديث، وأداة لإعادة تعريف الاستقلال في زمن العولمة الرقمية.

### 8.1 التحولات العالمية في مفهوم السيادة الرقمية

تبلور مفهوم السيادة الرقمية في صيغ متعددة تعكس الخصوصيات السياسية والاقتصادية والأمنية لكل دولة أو تكتل إقليمي. وأصبح مرتبطا بالقدرة على التحكم في **تدفّق البيانات والمعرفة** وإدارة البنى التحتية الرقمية

**الاتحاد الأوروبي: السيادة عبر حماية البيانات**

أطلق الاتحاد الأوروبي مشروع GAIA-X كإطار استراتيجي يهدف إلى بناء استقلالية رقمية أوروبية قادرة على تقليل الاعتماد على الشركات الأمريكية والصينية المسيطرة على خدمات الحوسبة السحابية. ويستند هذا المشروع إلى **اللائحة العامة لحماية البيانات** (GDPR) بوصفها حجر الزاوية في مقاربة أوروبية تضع حماية الخصوصية وحقوق الأفراد في قلب السيادة الرقمية. إنّ الاتحاد الأوروبي لا ينظر إلى السيادة الرقمية من زاوية أمنية فقط، بل يراها شرطًا لتعزيز الثقة في الاقتصاد الرقمي وحماية تنافسية الشركات الأوروبية في مواجهة عمالقة التكنولوجيا العالميين.

**الصين: نموذج السيطرة السيادية الكاملة**

على النقيض، تبنّت الصين مقاربة أكثر **انغلاقًا وتحكمًا** من خلال ما يُعرف بـ "**جدار الحماية العظيم**(Great Firewall) "، الذي يفرض سيطرة واسعة على حركة البيانات والمعلومات الداخلة والخارجة من فضائها الرقمي. هذه المقاربة لا تقتصر على البعد الأمني، بل تنسجم مع فلسفة سياسية ترى أن الحفاظ على الاستقرار الاجتماعي والسياسي يتطلب ضبطًا صارمًا لوسائل الاتصال والتدفق المعلوماتي. وقد أتاح هذا النموذج للصين تطوير منصاتها الرقمية المحلية (مثل WeChat و Alibabaو (Baiduلتصبح بدائل قوية للمنصات الغربية، مما عزز استقلاليتها التكنولوجية وسلطتها السيادية في المجال الرقمي.

**الولايات المتحدة: هيمنة المنصات والبنية التحتية**

أما الولايات المتحدة، فقد تمسكت بدور الهيمنة على **البنية التحتية الأساسية للإنترنت** من خلال السيطرة على عناوين بروتوكولات الإنترنت (IP) والهيئات التنظيمية الرئيسة مثل ICANN، فضلًا عن نفوذ شركات التكنولوجيا الكبرى المعروفة بـ .(GAFAM: Google, Apple, Facebook, Amazon, Microsoft)هذا النموذج لا يقوم على الانغلاق أو الحماية الصارمة كما في الصين، بل على **التوسع العالمي للمنصات الرقمية** بما يعكس فلسفة السوق المفتوحة والهيمنة الاقتصادية. ومع ذلك، فقد بدأ الخطاب الأمريكي في السنوات الأخيرة يشهد تحولات نتيجة تصاعد المخاطر السيبرانية، مما دفع إلى تبني سياسات أكثر تحفظًا تجاه الصين وروسيا في مجالات الذكاء الاصطناعي والبنية التحتية لشبكات الجيل الخامس.

**الأمم المتحدة: محاولة التوازن بين الانفتاح والسيادة**

على الصعيد الدولي، برزت جهود الأمم المتحدة في **المنتدى العالمي لحوكمة الإنترنت**(IGF) ، وفي النقاشات المتعلقة بوضع معايير دولية لإدارة الفضاء السيبراني. تسعى هذه الجهود إلى إيجاد **توازن بين مبدأ الانفتاح الرقمي** الذي يشكل أساس تطور الإنترنت، وبين **الاعتبارات السيادية للدول** التي ترى في هذا الفضاء عنصرًا مرتبطًا بالأمن القومي. ورغم أهمية هذه المبادرات، إلا أنها تواجه تحديات مرتبطة بالتباين الكبير في مصالح الدول الكبرى، مما يجعل الوصول إلى إطار عالمي ملزم أمرًا معقدًا للغاية.

إنّ هذه النماذج المختلفة تكشف أن مفهوم السيادة الرقمية ليس ثابتًا أو موحّدًا، بل هو **متغير تبعًا للسياق** .ففي أوروبا، يتجسد في حماية الحقوق الفردية والخصوصية

كجزء من هوية سـياسـية وقانونية؛ وفي الصـين، يتمحور حول **التحكم والسـيطرة** لضمان الاستقرار الداخلي؛ بينما يظهر في الولايات المتحدة في صورة **هيمنة اقتصادية وتكنولوجية عالمية**؛ أما الأمم المتحدة فتسعى إلى صياغة **حوكمة تشاركية** تحافظ على الطابع المفتوح للإنترنت مع مراعاة مصالح الدول.

هذه التباينات تعكس أن السيادة الرقمية ليست مجرد قضية تقنية، بل هي نتاج تفاعل بين **التاريخ السياسي، والمصالح الاقتصادية، والضرورات الأمنية** لكل دولة. وبذلك، يصبح الفضاء الرقمي مجالًا جديدًا لإعادة تعريف معنى الاستقلال والسيادة في النظام الدولي.

## 8.2 التجربة الأردنية – بين الاستجابة والتحول

في السـياق الأردني، تبرز جهود واضـحة لبناء بيئة سـيبرانية وطنية قادرة على مواجهة المخاطر والتحديات الرقمية المتزايدة. فقد أدركت الدولة منذ وقت مبكر أن التحول الرقمي لا يمكن أن يكتمل دون بنية صـلبة للأمن السـيبراني، الأمر الذي انعكس في جملة من المبادرات المؤسسية والقانونية والأكاديمية.

### المركز الوطني للأمن السيبراني

يُعَدّ المركز الوطني للأمن السـيبراني الذي أُنشـئ عام 2019 نقطة الارتكاز الرئيسة في حماية البنية الرقمية الوطنية. ويضطلع المركز بمهام متعددة تشمل وضع السـياسـات العامة، التنسـيق بين المؤسـسـات الحكومية والخاصـة، وتطوير آليات الاسـتجابة للحوادث السـيبرانية (National Cyber Security Center, 2021). كما يعمل على بناء قدرات فنية متقدمة لمواجهة التهديدات المتزايدة التي تستهدف البنى التحتية الحيوية مثل الطاقة والمصارف والاتصالات.

### الأطر القانونية والسياسات الوطنية

إلى جانب البنية المؤسسية، خطت الأردن خطوات تشريعية مهمة في هذا المجال. فقد جرى تحديث قانون الجرائم الإلكترونية بما يواكب تطور أشكال التهديد الرقمي، كما أُطلقت الاستراتيجية الوطنية للأمن السيبراني 2018–2023، التي وضعت أهدافًا استراتيجية لتعزيز الجاهزية الوطنية، وبناء منظومة استجابة متكاملة، وتطوير الوعي المجتمعي بمخاطر الفضاء الرقمي (Jordanian Government, 2018). هذه الأطر تمثل إطارًا قانونيًا وسياسيًا يوفر الحد الأدنى من الحماية، لكنها بحاجة مستمرة إلى مراجعة دورية لمواكبة التغيرات السريعة في البيئة الرقمية.

### الدور الأكاديمي والتعليمي

لم تقتصر الجهود على المستوى المؤسسي والتشريعي، بل شملت أيضًا القطاع الأكاديمي. فقد بدأت الجامعات الأردنية بإنشاء برامج متخصصة في الأمن السيبراني على مستوى البكالوريوس والدراسات العليا، بهدف تزويد السوق بخبرات محلية مؤهلة قادرة على مواجهة التحديات الأمنية (Al-Kasasbeh & Alsmadi, 2020). هذا الاستثمار في رأس المال البشري يشكل عنصرًا أساسيًا في بناء سيادة رقمية مستدامة، نظرًا لاعتمادها على الكفاءات الوطنية المؤهلة.

### التحديات المحلية

رغم هذه الإنجازات، تواجه الأردن تحديات سيبرانية متنامية. فقد شهدت قطاعات حيوية مثل البنوك والطاقة محاولات متكررة لاختراق أنظمتها، مما يعكس ارتفاع مستوى المخاطر الموجهة ضد البنية التحتية الوطنية (Shraim, 2021). كما

أن محدودية الموارد المالية والتقنية تمثل عائقًا أمام بناء أنظمة متكاملة تضاهي ما هو قائم في الدول المتقدمة.

**نحو التحول من الاستجابة إلى القرار الاستباقي**

يمكن القول إن الجهود الأردنية أسست لمرحلة الاستجابة للحوادث عبر تطوير الهياكل المؤسسية والتشريعية، إلا أن التحدي الأكبر يكمن في الانتقال نحو صناعة القرار الاستباقي .ويتطلب ذلك صياغة إطار سيادي شامل يعزز القدرة على التنبؤ بالتهديدات، وتوجيه الموارد، وبناء منظومة قرار سيبراني تتكامل فيها الأبعاد التقنية والسياسية والقانونية.

### 8.3 خارطة طريق تنفيذية – بناء منظومة قرار سيادي خلال 90 يومًا

لم يعد ممكنًا الاكتفاء بردود الفعل المتأخرة أمام التهديدات السيبرانية التي تطرق أبواب الدول بلا إنذار. ففي كل دقيقة، تتعرض البنى التحتية الحيوية لمحاولات اختراق، وتختبر المؤسسات قدرتها على الصمود، بينما يقف القرار الوطني أحيانًا في موقع المتأثر لا الفاعل. من هنا، تنبع الحاجة إلى خارطة طريق تنفيذية واضحة، تمتد على مدى تسعين يومًا، لتعيد تعريف القرار السيبراني بوصفه قرارًا سياديًا استباقيًا لا مجرد استجابة طارئة.

تهدف هذه الخارطة إلى تحويل الجهود المبعثرة إلى منظومة متكاملة، تتجسد في غرفة قرار سيادي تعمل كالعقل المركزي للدولة في الفضاء الرقمي. فهي تسعى إلى بناء قدرة وطنية قادرة على التنبؤ بالتهديدات قبل وقوعها، وتوجيه الموارد بسرعة ودقة، وربط مؤسسات الدولة والقطاعات الحيوية ضمن شبكة واحدة متناسقة. وبهذا، تتحول التشريعات والسياسات من نصوص مكتوبة إلى أدوات عملية، وتُقاس النتائج بمؤشرات أداء واضحة تضع الدولة أمام مرآة قدراتها الحقيقية.

الغاية ليست فقط حماية الأنظمة الرقمية، بل أيضًا تعزيز ثقة المواطن والمؤسسات في قدرة الدولة على حمايتهم، وإرساء نموذج وطني يمكن تطويره وتصديره كمرجعية إقليمية في مجال السيادة الرقمية. إنّ هذه الخارطة، بجدولها الزمني المكثف، تمثل إعلانًا بأن القرار الوطني لم يعد ينتظر الأزمة كي يتشكّل، بل يصنع بيئته بنفسه، ويستبق الخطر قبل أن يولد.

**المرحلة الأولى (الأيام 1 – 30): التأسيس والتحليل**

تمثّل هذه المرحلة **القاعدة الصلبة** التي يُبنى عليها المشروع السيادي بأكمله. فهي تركز على تأسيس الإطار المؤسسي الأولي، وفهم الواقع الرقمي الوطني بعمق، ورسم خريطة دقيقة للمخاطر. يمكن تقسيمها إلى أربعة محاور رئيسة:

**1. تشكيل الفريق الوطني متعدد التخصصات**

تبدأ المرحلة بتشكيل فريق وطني سيبراني يضم خبراء من مجالات متعددة:

- التقنيون :مهندسو الشبكات، مختصو أمن المعلومات، محللو التهديدات.
- القانونيون :خبراء في التشريعات الرقمية، الملكية الفكرية، قوانين الجرائم الإلكترونية.
- الإداريون :مسؤولون عن إدارة الأزمات والتنسيق المؤسسي وصناعة القرار.

هذا التنوع ضروري لأن السيادة الرقمية لا تُدار بزاوية واحدة؛ فهي منظومة معقدة تتشابك فيها التقنية مع القانون والسياسة. ويُناط بالفريق وضع دليل إجراءات أولي يوضح آليات العمل والتنسيق بين الأعضاء والجهات المعنية.

**2. التقييم الشامل للوضع الراهن**

بعد تشكيل الفريق، تُجرى عملية تقييم شامل للبنية التحتية الرقمية على المستويين الحكومي والخاص. ويشمل ذلك:

- مراجعة جاهزية الشبكات الوطنية وأنظمة الاتصالات.
- تحليل مستوى الحماية في القطاعات الحيوية: الطاقة، البنوك، النقل، الصحة.
- قياس قدرة المؤسسات على الاستجابة للحوادث الرقمية السابقة.

يتم ذلك باستخدام أدوات تحليل متقدمة مثل أنظمة Vulnerability Assessmentوبرمجيات SIEMلرصد الثغرات والهجمات. والغاية ليست فقط تشخيص المشكلات، بل أيضًا تحديد أولويات الإصلاح.

**3. رسم خريطة المخاطر الرقمية**

بناءً على نتائج التقييم، يتم إعداد خريطة وطنية للمخاطر السيبرانية .هذه الخارطة توضح:

- المواقع الأكثر عرضة للهجمات.
- نوعية التهديدات (هجمات مالية، تجسس إلكتروني، هجمات تعطيل).
- مستوى الخطورة (مرتفع، متوسط، منخفض).
- التكرار الزمني للهجمات السابقة.

تُعرض الخارطة بطريقة بصرية واضحة (ألوان، رموز، مؤشرات) بحيث تصبح أداة تشغيلية تُستخدم في غرفة القرار السيبراني.

**4. إطلاق غرفة قرار سيبرانية مصغّرة(Pilot)**

كخطوة عملية، يتم إنشـــاء غرفة قرار مصـــغّرة تُعد بمثابة نموذج أولي (Pilot) لتجريب آليات العمل.

- يتم فيها محاكاة هجمات بسيطة لرصد الاستجابة.
- اختبار قنوات الاتصال بين المؤسسات.
- وضع آليات أولية لتبادل المعلومات وتوحيد التقارير.

الهدف من هذه الغرفة ليس الحل النهائي، بل بناء مختبر عملي يمنح الفريق خبرة مباشرة ويُظهر نقاط الضعف في التنسيق قبل الانتقال إلى مرحلة البناء والتمكين.

**خلاصة المرحلة الأولى**

بنهاية الأيام الثلاثين الأولى، تكون الدولة قد:

1. كوّنت فريقًا وطنيًا متكاملاً.
2. امتلكت تقييمًا واقعيًا لحالتها الرقمية.
3. رسمت خريطة شاملة للمخاطر.
4. أطلقت نواة غرفة قرار سيبرانية.

وبذلك، تنتقل من مرحلة الرصد غير المنظم إلى مرحلة التحليل الممنهج والتجريب العملي، وهو ما يُمهِّد الطريق للانتقال إلى المرحلة الثانية :البناء والتمكين.

**المرحلة الثانية (الأيام 31 – 60): البناء والتمكين**

بعد أن أرست المرحلة الأولى الأساس عبر تشكيل الفريق الوطني ورسم خريطة المخاطر الرقمية وإطلاق غرفة القرار المصغّرة، تأتي المرحلة الثانية لتنتقل من التشخيص والتجريب إلى **البناء المؤسسي والتمكين التشغيلي** .هذه المرحلة تمثل النقطة التي يبدأ فيها القرار السيبراني بالتحول من فكرة إلى منظومة متكاملة تعمل وفق قواعد واضحة وإجراءات معيارية.

**1. اعتماد نموذج القرار السيادي**

الخطوة الأولى في هذه المرحلة هي صياغة واعتماد نموذج القرار السيادي الذي يُعدّ المرجعية المركزية لعمل المنظومة. يقوم النموذج على خمس حلقات مترابطة:

1. الرصد :جمع البيانات بشكل لحظي من مختلف المؤسسات والقطاعات.
2. التحليل :معالجة هذه البيانات عبر أدوات استخبارات التهديدات (Threat Intelligence)وتوظيف الذكاء الاصطناعي للكشف المبكر عن الأنماط.
3. القرار :انتقال المعلومة المحللة إلى صناع القرار السياديين لاتخاذ إجراء محدد.
4. التنفيذ :تطبيق القرارات عبر المؤسسات المعنية بشكل منسق.
5. المراجعة :تقييم الاستجابة وتصحيح المسار لضمان التعلم المستمر.

هذا النموذج يضمن أن القرار لم يعد رد فعل فرديًا أو مؤقتًا، بل عملية سيادية مؤسسية تتسم بالاستمرارية والتكامل.

### 2. إعداد سياسات قطاعية للأمن السيبراني

نظرًا لاختلاف طبيعة المخاطر بين القطاعات (البنوك، الطاقة، الصحة، النقل)، تُعدّ **سياسات قطاعية متخصصة** تُكمل السياسات الوطنية العامة.

- في القطاع المالي: التركيز على أنظمة الدفع الإلكترونية ومكافحة الاحتيال.
- في قطاع الطاقة: حماية أنظمة التحكم الصناعي.(SCADA)
- في قطاع الصحة: صون البيانات الطبية وحماية الخصوصية.

هذه السياسات تُترجم الخطة الوطنية إلى تعليمات تنفيذية متناسبة مع طبيعة كل قطاع، وتُسهم في رفع مستوى التنسيق بين الدولة والقطاع الخاص.

### 3. إنشاء مركز وطني للإنذار المبكر

يُطلق في هذه المرحلة مركز وطني للإنذار المبكر يُمثل العين الساهرة على الفضاء السيبراني. يتولى المركز:

- مراقبة الأنشطة الرقمية المشبوهة محليًا وإقليميًا ودوليًا.
- إرسال تنبيهات لحظية للمؤسسات عند رصد تهديدات ناشئة.
- ربط البيانات المحلية بمصادر استخبارات التهديدات العالمية لتوسيع نطاق الرؤية.

وبذلك، يصبح لدى الدولة نظام يتيح التحذير قبل وقوع الهجوم، بدلًا من الاكتفاء بالاستجابة بعد فوات الأوان.

**4. تنفيذ محاكاة عملية**(Red vs Blue Team)

لتجريب فاعلية المنظومة، يتم تنفيذ **تمارين محاكاة عملية** عبر فرق Red Team (المهاجمين) و Blue Team(المدافعين).

- يقوم فريق "الأحمر" بمحاكاة هجوم سيبراني واقعي يستهدف قطاعًا محددًا.
- يتولى فريق "الأزرق" الدفاع باستخدام الأدوات والآليات الموضوعة.
- في نهاية التمرين، يُجرى تقييم شامل لسرعة الاستجابة ودقة القرارات والقدرة على التنسيق بين المؤسسات.

هذا التمرين العملي لا يكشف فقط عن نقاط الضعف التقنية، بل يختبر أيضًا **كفاءة منظومة القرار** وقدرتها على التحرك تحت الضغط.

**5. صياغة "الميثاق السيادي الرقمي الأردني"**

تُختتم المرحلة الثانية بإعلان "الميثاق السيادي الرقمي الأردني"، وهو وثيقة مرجعية تُحدد المبادئ العامة للسيادة الرقمية في الأردن. يتضمن الميثاق:

- التزام الدولة بحماية فضائها الرقمي كجزء من أمنها الوطني.
- مبدأ استقلالية القرار السيبراني عن الضغوط الخارجية.
- إشراك جميع القطاعات في حماية الفضاء الرقمي.

• ترسيخ الثقة بين الدولة والمجتمع من خلال الشفافية والمسؤولية.

الميثاق هنا ليس مجرد نص سياسي أو قانوني، بل إطار هوياتي يعكس خصوصية التجربة الأردنية ويضعها في سياق عالمي.

**خلاصة المرحلة الثانية**

بنهاية هذه المرحلة، تكون الدولة قد:

1. اعتمدت نموذجًا سياديًا متكاملاً لصناعة القرار.
2. طوّرت سياسات قطاعية تعالج خصوصية التهديدات.
3. أنشأت مركزًا وطنيًا للإنذار المبكر.
4. اختبرت قدراتها عبر محاكاة عملية واقعية.
5. صاغت ميثاقًا سياديًا رقميًا يرسّخ الهوية الوطنية في الفضاء السيبراني.

وبذلك، تنتقل التجربة الأردنية من مرحلة التشخيص والتجريب إلى مرحلة **البناء والتمكين**، تمهيدًا للانتقال في المرحلة الثالثة إلى التشغيل والاستدامة.

**المرحلة الثالثة (الأيام 61 – 90): التشغيل والاستدامة**

مع اكتمال مرحلتي التأسيس والتحليل، ثم البناء والتمكين، تصل خارطة الطريق إلى لحظة الاختبار الحقيقي :تشغيل المنظومة بكامل طاقتها وتحويلها من مشروع تجريبي إلى واقع مؤسسي مستدام. تمثل هذه المرحلة الإعلان الفعلي عن ولادة منظومة القرار السيادي الوطنية، بوصفها أداة يومية لإدارة الفضاء الرقمي وحماية السيادة الوطنية.

### 1. تشغيل غرفة القرار السيادي الوطنية

في هذه المرحلة، تُفتتح غرفة القرار السيادي الوطنية بحضور كامل للكوادر المؤسسية والتقنية، وتبدأ بالعمل على مدار الساعة (24/ 7). تتحول الغرفة من نموذج مصغّر إلى مركز سيادي متكامل مجهز بشاشات رصد، منصات تحليل، وقنوات اتصال مباشرة مع القطاعات الحيوية. هنا يصبح القرار السيبراني فعلًا سياديًا متواصلًا، لا رد فعل طارئًا.

### 2. إصدار التقرير السيادي الوطني الأول

كأحد أبرز مخرجات هذه المرحلة، يُصدر الفريق الوطني التقرير السيادي الوطني الأول للأمن السيبراني .يتضمن التقرير:

- ملخصًا عن الوضع الرقمي الوطني.
- نتائج تقييم التهديدات خلال فترة التنفيذ.
- الدروس المستفادة من المحاكاة والتجارب.
- توصيات عملية لتعزيز الاستعداد المستقبلي.

إصدار هذا التقرير يمثل شفافية مؤسسية، ويُظهر أن المنظومة لا تكتفي بالعمل الداخلي، بل تُنتج معرفة استراتيجية قابلة للتوظيف في صنع القرار الوطني.

### 3. إطلاق منصة شراكة وطنية

تعتمد المنظومة على مبدأ أن الأمن السيبراني ليس مسؤولية الدولة وحدها، بل هو مسؤولية مشتركة. لذلك، يتم في هذه المرحلة إطلاق منصة شراكة وطنية تجمع بين:

- الحكومة ومؤسساتها الأمنية والتنظيمية.
- القطاع الخاص، وخاصة البنوك، شركات الطاقة، وشركات الاتصالات.
- الجامعات ومراكز البحث العلمي.

تهدف المنصة إلى تبادل المعلومات والخبرات، وتنظيم تدريبات مشتركة، وتعزيز ثقافة الأمن السيبراني المجتمعي. فهي تُحوّل السيادة الرقمية من مشروع حكومي ضيق إلى مشروع وطني شامل.

### 4. اعتماد إطار وطني للاستجابة للحوادث السيبرانية

لتأمين استدامة العمل، يتم إقرار إطار وطني موحد للاستجابة للحوادث السيبرانية .(National Incident Response Framework)يحدد هذا الإطار:

- أدوار ومسؤوليات كل جهة في حال وقوع هجوم.
- مسارات الاتصال والتنسيق.
- آليات التوثيق والإبلاغ والتحقيق.

وبهذا، تُصبح الاستجابة للحوادث ليست فعلًا عشوائيًا، بل عملية منظمة ومؤسسية تضمن سرعة التحرك وتقليل الأضرار.

### 5.التقييم الدوري كل 15 يومًا

وأخيرًا، تُرسخ هذه المرحلة مبدأ التحسين المستمر عبر إجراء تقييم دوري نصف شهري (كل 15 يومًا) يقيس أداء المنظومة باستخدام مؤشرات واضحة مثل:

- سرعة الاستجابة للهجمات.
- نسبة التهديدات المكتشفة مبكرًا.
- مستوى التنسيق بين المؤسسات.
- مدى فعالية الإنذار المبكر.

هذه التقييمات لا تُعد مجرد تقارير داخلية، بل آلية تصحيحية تُبقي المنظومة في حالة جاهزية عالية، وتمنع تراكم الأخطاء أو القصور.

**خلاصة المرحلة الثالثة**

بنهاية هذه المرحلة، تكون الدولة قد انتقلت من مرحلة التأسيس والتجريب إلى مرحلة التشغيل والسيادة الفعلية .فقد أصبحت تمتلك غرفة قرار سيادي فاعلة، وآلية شفافة للإفصاح عن التهديدات، ومنصة وطنية للشراكة، وإطارًا مؤسسيًا للاستجابة، ونظامًا دوريًا للتقييم والتحسين المستمر.

إنها المرحلة التي يتحول فيها المشروع من "خطة على الورق" إلى منظومة سيادية حية تعمل على مدار الساعة، وتمنح الأردن قدرة حقيقية على الاستباق وصناعة القرار في فضاء رقمي لا يعرف الانتظار.

**عناصر نجاح التجربة الأردنية**

لا يمكن لأي خارطة طريق تنفيذية أن تحقق أهدافها دون توافر عناصر نجاح جوهرية تدعم المسار وتضمن استدامته. وفي الحالة الأردنية، تتجسد هذه العناصر في أربعة محاور مترابطة:

### 1. الإرادة السياسية العليا

تُعَدّ الإرادة السياسية حجر الزاوية لأي مشروع سيادي. فنجاح المنظومة يتطلب التزامًا واضحًا من أعلى مستويات صنع القرار في الدولة، بما يوفّر الغطاء القانوني والمالي والمؤسسي لتنفيذ الخطوات اللازمة. الإرادة السياسية هنا ليست مجرد إعلان نوايا، بل هي إرادة مُلزِمة تُترجم إلى سياسات وتشريعات وقرارات داعمة.

### 2. بناء القدرات البشرية

الركيزة الثانية هي الإنسان، إذ لا يمكن بناء سيادة رقمية بموارد تقنية فقط دون الاستثمار في رأس المال البشري. ويشمل ذلك:

- تطوير برامج تدريبية متخصصة لموظفي المؤسسات الحكومية والقطاعات الحيوية.
- إدماج الأمن السيبراني في المناهج الجامعية والدراسات العليا.
- تشجيع البحث العلمي في مجالات مثل الذكاء الاصطناعي الدفاعي، والتحليل السلوكي، ونماذج القرار السيبراني.

بهذا، يتحول المجتمع الأكاديمي والمهني إلى حاضنة للخبرة الوطنية بدلًا من الاعتماد المفرط على الخبرات الخارجية.

### 3. الشراكات الإقليمية والدولية

لا يمكن لأي دولة، مهما بلغت إمكاناتها، أن تواجه التحديات السيبرانية بمعزل عن العالم. ومن هنا تبرز أهمية بناء شراكات إقليمية ودولية مع مراكز متقدمة في الأمن السيبراني. هذه الشراكات تتيح:

- تبادل المعلومات حول التهديدات الناشئة.
- الاستفادة من أفضل الممارسات العالمية.
- المشـــاركة في تدريبات ومحاكاة دولية (مثل Cyber Polygonو Locked Shields).

وبـذلـك، تتحول التجربـة الأردنيـة إلى جزء من منظومـة عـالميـة، دون أن تفقـد هويتها الوطنية.

**4. مؤشرات الأداء(KPIs)**

أخيرًا، لا يكتمل النجاح دون قياس الأداء .لذلك، ينبغي وضـــع مؤشـــرات أداء دقيقة وواضحة تشمل:

- سرعة الاستجابة للهجمات منذ لحظة الاكتشاف وحتى اتخاذ القرار.
- تقليل الخسائر المالية والتشغيلية الناتجة عن الحوادث السيبرانية.
- تعزيز ثقة المواطن في قدرة الدولة على حماية بياناته وخدماته الرقمية.

هذه المؤشرات تتيح تقييمًا موضوعيًا للمنظومة، وتوفر قاعدة للتطوير والتحسين المستمر.

إنّ نجاح التجربة الأردنية في بناء منظومة قرار ســيادي رقمي لا يعتمد على التقنية وحدها، بل على التقاء الإرادة الســياســية، وتنمية الكفاءات البشــرية، والانفتاح على الشــراكات الدولية، واعتماد نظام صــارم لقياس الأداء .هذه العناصــر مجتمعة تشــكل الضــمانة الحقيقية لاســتدامة المشــروع وتحويله من خطة زمنية قصــيرة المدى إلى إستراتيجية وطنية راسخة.

وبالإضـــافة لذلك فإنّ نجاح الأردن في بلورة خارطة طريق تنفيذية لبناء منظومة قرار ســـيادي خلال 90 يومًا يمثل تجربة نوعية قادرة على أن تتحول إلى نموذج إقليمي وعـالمي. فهـذا الإنجاز لا يعكس فقط القـدرة على التكيّف مع التحـديات الكونية، بل يبرهن أيضًا على إمكانية التحول من الهشاشة إلى القوة، ومن التبعية إلى الاستقلال، حين تتكامل الإرادة السياسية مع الكفاءات البشرية والأطر المؤسسية.

وبهذا، تتحقق معادلة دقيقة: التوازن بين التحديات الكونية التي يفرضـها الفضـاء الرقمي من جهة، والنماذج الوطنية التي تنبع من خصـــوصـــية كل مجتمع من جهة أخرى. ومن هنا، تكتمل رســـالة هذا الكتاب: أنّ القرار الســـيبراني ليس مجرد تقنية عابرة أو أداة دفاعية، بل هو أفق ســـيادي يعيد رســـم معنى الدولة في العصـــر الرقمي، ويجعلها قادرة على صياغة مصيرها لا أن تكون رهينة لمعادلات الآخرين.

### 8.4 أين يقف الأردن في مسار السيادة الرقمية؟

تبرز التجربة الأردنية اليوم كإحدى الحالات التي تســـتحق التوقف عندها والدراســـة المتأنية. فبرغم محدودية الموارد المالية والتقنية، أدركت المملكة مبكرًا أن مســـتقبلها الرقمي لا يمكن أن يتشـــكل من خلال مبادرات متناثرة أو ردود أفعال ظرفية، بل عبر منظومة متكاملة للســـيادة الســـيبرانية قادرة على اســـتباق التحديات وحماية الفضاء الوطني.

وفي هذا السياق، جاء تأسيس المركز الوطني للأمن السيبراني عام 2019 ليكون نقطة الارتكاز الرئيســـة في صـــون البنية الرقمية الوطنية وبناء قدرات الدولة في المواجهة .(National Cyber Security Center, 2021) وقد تعزز هذا المســـار بإطلاق الاســـتراتيجية الوطنية للأمن الســـيبراني 2018–2023، ثم الانتقال إلى

الاســتراتيجية الثانية 2024–2028 التي وضــعت معالم طريق أطول مدى لتعزيز القدرات المحلية وتوســيع دائرة الفاعلية الســيبرانية (Jordanian Government, 2018; Jordan Times, 2024).

كما أدركت الدولة أن بناء الســيادة الرقمية لا يتحقق فقط عبر التشــريعات والمؤسسات، بل يحتاج إلى رأس مال بشري مؤهل، فشرعت الجامعات الأردنية في إنشــاء برامج أكاديمية متخصصــة في الأمن الســيبراني على مســتويات البكالوريوس والدراســات العليا. وقد أســهم ذلك في تأهيل جيل جديد من الخبرات الوطنية، قادر على مواكبة التحديات العالمية والانخراط في صياغة حلول مبتكرة (Al-Kasasbeh & Alsmadi, 2020).

وهكذا، يظهر النموذج الأردني بما يحمله من تحديات ونجاحات كمسار متدرج يؤكد أن الدول الصــغيرة أو محدودة الموارد ليســت عاجزة عن صــياغة ســيادتها الرقمية، بل قادرة على تحويل المحدودية إلى فرصة والتحدي إلى قوة إذا ما توفرت الرؤية والإرادة السياسية.

### 1. المركز الوطني للأمن السيبراني

يشكّل المركز الوطني للأمن السيبراني(NCSC) ، الذي أُنشئ عام 2019، أحد أبرز المنعطفات المؤسسية في مسيرة الأردن نحو ترسيخ سيادته الرقمية. فقد جاء تأســيســه اســتجابةً لحاجة وطنية متنامية إلى وجود جهة مركزية قادرة على تنســيق الجهود، صياغة السياسات، وإدارة المخاطر الرقمية التي أخذت في التزايد والتعقيد مع تسارع التحول الرقمي على المستويين الحكومي والخاص.

يتولى المركز أدوارًا محورية تتجاوز الجانب التشــغيلي إلى صــياغة رؤية وطنية شــاملة للأمن الســيبراني .فهو يضــع الســياســات العامة، ويعمل على رفع جاهزية

المؤسســات الوطنية، ويُشـرف على تطوير قدرات فنية متقدمة لمواجهة التهديدات التي تســتهدف قطاعات اســتراتيجية مثل الطاقة، المصــارف، الاتصــالات، والنقل (National Cyber Security Center, 2021).كما يمثّل حلقة وصــل بين مختلف الجهات، مما مكّنه من لعب دور قيادي في توحيد الاســتجابة الوطنية وتوجيهها وفق معايير موحدة.

وقد أسـهم إنشـاء المركز في إحداث نقلة نوعية على مستوى الإدارة السيبرانية في الأردن، إذ انتقل التعامل مع التهديدات من كونه جهدًا متفرقًا إلى كونه منظومة متكاملة تستند إلى مرجعية واحدة. وهذا التحول يعكس وعي الدولة بأهمية أن يكون الأمن السيبراني جزءًا من بنيتها السيادية، لا مجرد وظيفة تقنية هامشية.

### 2. الاستراتيجيات الوطنية والسياسات التشريعية

أدركت الحكومة الأردنية منذ وقت مبكر أن بناء فضـــاء رقمي آمن لا يمكن أن يُختزل في جدران تقنية أو حلول برمجية آنية، بل يتطلب إطارًا وطنيًا شاملًا يجمع بين الرؤية الاســتراتيجية والتشـريعات الفاعلة. ومن هذا الإدراك، جاءت الاســتراتيجية الوطنية للأمن السيبراني (2018–2023) بوصفها محطة تأسيسية، إذ وضعت أهدافًا طموحة لتعزيز الجاهزية الرقمية، ورفع مسـتوى الحماية، وتمكين المؤســسـات من التصـــدي للتهـديـدات المتزايـدة في محيط عـالمي ســريع التحوّل (Jordanian Government, 2018).

ومع اختتام تلك المرحلة، أعلنت المملكة عن الاســتراتيجية الجديدة للأعوام (2024–2028)، التي يمكن اعتبارهـا نقطـة انعطـاف في مسـيرة التحول الرقمي الأردني. فهي لا تكتفي بمتابعة مســار الحماية، بل تتجاوز ذلك إلى ترسـيخ بيئة ســيبرانية قائمة على القدرات الوطنية، وعلى شــراكة متينة بين الحكومة والقطاع

الخاص والجامعات، بما يجعل الأمن السـيبراني جزءًا أصـيلًا من مشـروع التنمية الشاملة للدولة.(Jordan Times, 2024)

إلى جانب هذه الجهود الاستراتيجية، خطت الدولة خطوات تشريعية مهمة، من أبرزها إقرار قانون الجرائم الإلكترونية (2023)، الذي جاء اسـتجابة لتطور أنماط الجرائم الرقمية عالميًا، وسـعيًا لمواءمة المنظومة الوطنية مع البيئة القانونية الدولية. وقد أثار القانون نقاشًـا واسـعًا بين من رأى فيه حصـنًا لحماية المجتمع من المخاطر الرقمية، ومن اعتبره مثيرًا للقلق من حيث احتمال تأثيره على حرية التعبير والحقوق الرقمية.(Wikipedia, 2023)

بهذا، يمكن القول إن التجربة الأردنية في بناء السـياسـات والتشـريعات الرقمية تعكس محاولة متواصـلة لتحقيق معادلة صـعبة: حماية الأمن الوطني من جهة، وصـون الحقوق والحريات العامة من جهة أخرى. إنها معادلة لا تخص الأردن وحده، بل تواجهها معظم دول العالم في زمن السيادة الرقمية والعولمة السيبرانية.

### 3. البنية المؤسسية JoCERT :كنموذج عملي

يشـكّل فريق الاسـتجابة للطوارئ الحاسـوبية الأردني (JoCERT) أحد الأعمدة المؤسسية الرئيسة في منظومة الأمن السيبراني الوطنية. وقد تأسس الفريق عام 2017 بوصفه الذراع التنفيذي المختص بالاستجابة للحوادث السيبرانية، مستجيبًا لحاجة ملحّة إلى وجود جهة متخصصة قادرة على التحرك السريع في حال وقوع اختراقات أو هجمات رقمية.(FIRST, 2023)

تتمثل مهام JoCERT في طيف واسع من الوظائف الحيوية، تشمل:

- الطب الشرعي الرقمي :تحليل الأجهزة والأنظمة المخترَقة لاستخلاص الأدلة الرقمية وتوثيقها بما يدعم التحقيقات القضائية.
- التنبيه المبكر :مراقبة الفضاء السيبراني ورصد التهديدات الناشئة محليًا وإقليميًا ودوليًا، وتزويد المؤسسات الوطنية بإنذارات سريعة حول المخاطر المحتملة.
- تقديم الاستشارات والتدريب :مساعدة المؤسسات الحكومية والخاصة على تعزيز قدراتها الوقائية والاستباقية، من خلال التوصيات الفنية وبرامج بناء القدرات.

وما يميز JoCERT ليس فقط دوره المحلي، بل أيضًا انفتاحه على الشراكات الدولية .فقد أصبح الفريق عضوًا رسميًا في شبكة OIC-CERTالتابعة لمنظمة التعاون الإسلامي، إلى جانب عضويته في المنتديات الدولية مثل .FIRSTهذه الشراكات تعكس إدراك الأردن أن الأمن السيبراني لا يمكن أن يُدار بمعزل عن النظام الدولي، وأن الانخراط في التعاون الإقليمي والدولي يوفّر مزيدًا من الحماية ويتيح الاستفادة من الخبرات المتقدمة.

وبذلك، يمكن النظر إلى JoCERT كنموذج عملي يترجم السياسات الوطنية إلى إجراءات تشغيلية ملموسة، ويجسد التوجه الأردني نحو الجمع بين الاستقلالية الوطنية والانفتاح على التعاون الدولي في مجال السيادة الرقمية.

### 4. البعد الأكاديمي والقدرات البشرية

لم يقتصر مسار الأردن في بناء سيادته الرقمية على تطوير البنية المؤسسية والتشريعية، بل امتد ليشمل القطاع الأكاديمي والتعليمي باعتباره الركيزة الأكثر

استدامة. فالوعي بأن الأمن السيبراني لا يُصان بالتقنيات وحدها، بل يحتاج إلى رأس مال بشري مؤهل، دفع الجامعات الأردنية إلى إطلاق برامج أكاديمية متخصصة في هذا المجال.

بدأت بعض الجامعات بتأسيس برامج للبكالوريوس في الأمن السيبراني، موجهة نحو تزويد الطلبة بالمعارف التقنية الأساسية في حماية الشبكات، التشفير، واختبار الاختراق. وتطورت هذه المبادرات لاحقًا لتشمل برامج للدراسات العليا (الماجستير والدكتوراه) تركز على الأبحاث التطبيقية في مجالات مثل الذكاء الاصطناعي للأمن السيبراني، التحليل السلوكي للتهديدات، وحماية أنظمة التحكم الصناعي.(Al-Kasasbeh & Alsmadi, 2020)

تشمل هذه البرامج موضوعات مثل حماية الشبكات، التشفير، اختبار الاختراق، التحليل الجنائي الرقمي، وصولًا إلى مجالات بحثية متقدمة مثل الذكاء الاصطناعي للأمن السيبراني وأنظمة التحكم الصناعي. كما بدأت الجامعات بتنظيم مختبرات متخصصة ومسابقات وطنية مثل Capture the Flag (CTF)، التي تحاكي بيئات التهديدات الواقعية وتكسب الطلبة مهارات عملية مباشرة.

كما أسهمت هذه البرامج في تشجيع الطلبة على إنتاج بحوث علمية ونشرها في مجلات دولية، الأمر الذي عزز حضور الأردن في النقاشات العالمية حول قضايا الأمن السيبراني والسيادة الرقمية .(Jordan Times, 2024) وبذلك، لم يعد التعليم الجامعي مجرد قاعات دراسية، بل تحوّل إلى منصة إبداعية وبحثية ترفد الدولة بالقدرات البشرية الوطنية وتضع الأردن في موقع متقدم على خارطة النقاش الدولي.

هذا التوجه يُظهر أن الأردن ينظر إلى التعليم والبحث العلمي ليس فقط كوسيلة لرفد سوق العمل بكفاءات، بل كجزء من إستراتيجية وطنية للسيادة الرقمية . فالاستثمار في الإنسان هو الاستثمار الوحيد القادر على ضمان الاستدامة، لأنه يخلق جيلًا من الخبراء المحليين الذين يستطيعون تطوير حلول أصلية تتناسب مع السياق الأردني، بدلًا من الاعتماد الدائم على الخبرات المستوردة.

وبذلك، يُمكن القول إن البعد الأكاديمي يشكل العمود الفقري لمشروع السيادة الرقمية الأردني؛ فهو يزوّد المنظومة بالعقول القادرة على الحماية والابتكار في آن واحد.

### 5. التحديات الراهنة

رغم الإنجازات التي حققها الأردن في مجال الأمن السيبراني، ما تزال هناك تحديات جوهرية تعيق الوصول إلى منظومة سيادية متكاملة.

فأول هذه التحديات يتمثل في تزايد الهجمات على القطاعات الحيوية مثل البنوك والطاقة، حيث كشفت هذه الحوادث عن هشاشة البنية التحتية الرقمية في بعض المواقع الحساسة .(Shraim, 2021) ويكمن الحل هنا في تطوير أنظمة دفاعية متقدمة تستند إلى الرصد اللحظي، وإلى تعزيز التعاون مع مراكز استخبارات التهديدات الإقليمية والدولية، بحيث لا تبقى المؤسسات وحدها في مواجهة تهديدات عابرة للحدود.

أما التحدي الثاني، فهو محدودية الموارد المالية والتقنية، التي قد تُبطئ وتيرة التطوير مقارنة بدول أكثر تقدمًا. غير أن هذا القيد يمكن تحويله إلى فرصة عبر التركيز على بناء القدرات البشرية والاعتماد على الكفاءات المحلية، وتشجيع

البحث العلمي في الجامعات لتقديم حلول منخفضة الكلفة ومرتبطة بالسياق الوطني. فالقوة هنا لا تُقاس بكمية الأموال المرصودة فقط، بل بقدرة الدولة على تحويل المعرفة إلى أدوات عملية.

ويبرز أيضًا تحدٍ ثالث يتمثل في غياب إطار وطني متكامل للاستجابة السيبرانية يغطي كل القطاعات بآليات تشغيلية واضحة. فوجود JoCERT والإطار الوطني العام خطوة مهمة، لكنها تظل غير كافية دون ربط القطاعات الحيوية ضمن منظومة موحدة تتيح تبادل المعلومات بشكل فوري، وتحدد بوضوح المسؤوليات عند وقوع أي حادث. إن الحل يكمن في تصميم بروتوكولات استجابة وطنية تجعل من الهجوم السيبراني حدثًا مُدارًا ومسيطرًا عليه، لا أزمة متفرقة تُعالج كل مرة بشكل منفصل.

أما التحدي الرابع، فيتعلق بـ ضعف المشاركة المؤسسية المشتركة بين الحكومة والقطاع الخاص والجامعات، وهو ما يحدّ من إمكان صياغة منصة سيادية متكاملة. والحل هنا هو إطلاق شراكات وطنية فاعلة تجعل من الأمن السيبراني مسؤولية جماعية، بحيث تُسهم الشركات بتجربتها التقنية، والجامعات بأبحاثها المتقدمة، والحكومة بقدرتها التنظيمية. عندها يتحول المشروع من جهد حكومي إلى مشروع وطني شامل.

وبذلك، يتضح أن التحديات الراهنة ليست نهاية الطريق، بل بدايات للتحول . فهي تكشف الثغرات التي تحتاج إلى معالجة، وتفتح في الوقت ذاته بابًا واسعًا للحلول الإبداعية التي يمكن أن تجعل التجربة الأردنية في السيادة الرقمية نموذجًا إقليميًا رائدًا.

**لتجاوز التحديات الراهنة وتعزيز المكتسبات المحققة، يحتاج الأردن إلى رسم ملامح مستقبلية واضحة لمسار سيادته الرقمية، وذلك من خلال التحرك في اتجاهين متوازيين ومتكاملين.**

**الاتجاه الأول: ترسيخ البنية الحالية**

يقوم هذا الاتجاه على تعزيز ما تم إنجازه عبر تطوير غرفة قرار سيادي متكاملة، تعمل كعقل مركزي لإدارة المشهد السيبراني لحظيًا. هذه الغرفة ينبغي أن تمتلك قدرات متقدمة في الرصد، التحليل، واتخاذ القرار، بحيث تتحول من مجرد وحدة للتنسيق إلى منصة استراتيجية لصناعة القرار السيبراني الوطني. كما يتطلب الأمر إنشاء مركز وطني للإنذار المبكر، قادر على التنبؤ بالهجمات قبل وقوعها، عبر الاعتماد على تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة. وإلى جانب ذلك، فإن صياغة إطار وطني موحد للاستجابة للحوادث السيبرانية تمثل خطوة ضرورية لضمان سرعة التنسيق بين القطاعات، وتحويل الاستجابة من فعل متفرق إلى عملية مؤسسية منظمة.

**الاتجاه الثاني: بناء نموذج وطني ملهم**

الطموح الأكبر يتمثل في بلورة "الميثاق السيادي الرقمي الأردني"، وهو إطار جامع يدمج بين الدولة، القطاع الخاص، والجامعات في شراكة وطنية متكاملة. يقوم هذا الميثاق على مبدأ أن حماية الفضاء الرقمي لا يمكن أن تكون مسؤولية حكومية بحتة، بل يجب أن تتحول إلى مسؤولية جماعية تشمل كل مكونات المجتمع. هذا التوجه يتسق مع تجارب دول متقدمة مثل إستونيا، التي حققت نجاحًا بارزًا في بناء

نموذج للسـيادة الرقمية عبر دمج الأطر الحكومية بالتعاون مع القطاع الأكاديمي والخاص.(Tikk, 2019)

**عناصر القوة الداعمة للطموحات الأردنية**

يمتلك الأردن بالفعل مجموعة من عناصر القوة الاستراتيجية التي تؤهله للانتقال من مرحلة الاستجابة إلى الريادة.

- أولًا :الموقع الجغرافي الذي يربط المشرق العربي بالعالم، مما يجعله نقطة عبور رقمية يمكن تطويرها لتصبح مركزًا إقليميًا للبيانات والخدمات السيبرانية (World Bank, 2020).
- ثانيًا :التنوع الاجتماعي والثقافي، الذي يعزز من فرص الابتكار ويخلق بيئة خصبة للأفكار الجديدة.
- ثالثًا :الرأسمال البشري الشاب، حيث يشكّل الشباب غالبية سكان الأردن، وهو ما يُعدّ مصدرًا استراتيجيًا للطاقة الإبداعية في مجال التكنولوجيا والأمن السيبراني.(Jordan Department of Statistics, 2022)

**التكامل بين الإرادة السياسية والإطار المؤسسي**

غير أن تحويل هذه العناصر إلى ميزة تنافسية وطنية يتطلب توافر إرادة سياسية عليا تمنح الأمن السيبراني أولوية استراتيجية في سياسات الدولة، وتُرفده بالموارد اللازمة. كما يحتاج إلى تطوير إطار مؤسسي مرن وفعّال قادر على استيعاب المتغيرات العالمية السريعة، ويضمن في الوقت ذاته التكامل بين التشريعات، المؤسسات، والشركاء المحليين والدوليين.

إن الجمع بين هذه العناصر يُمكّن الأردن من أن يتحول إلى نموذج إقليمي متقدم في مجال السـيادة الرقمية، لا سـيما في بيئة شـرق أوسـطية ما تزال في طور بناء اسـتراتيجياتها الرقمية. وبهذا، يمكن للمملكة أن تنتقل من موقع "المتلقي" للتقنيات والسـياسـات إلى موقع "المبادر" وصـانع الرؤية، بما يعزز اسـتقلاليتها السـيادية في عالم تُدار فيه القوة عبر البيانات والخوارزميات أكثر مما تُدار عبر الحدود والجيوش.

## خاتمة الفصل

يبيّن هذا الفصل أن السيادة الرقمية لم تعد هامشًا تقنيًا في كتب الإدارة العامة، بل أصبحت مكوّنًا سياديًا يعيد تعريف معنى الدولة في عصر تتداخل فيه الحدود المادية بالحدود الخوارزمية. فالنماذج العالمية – الأوروبية القائمة على حماية البيانات، والصينية المرتكزة إلى السيطرة السيادية، والأمريكية التي تُهيمن عبر المنصات والبنى التحتية، والمساعي الأممية نحو توازن الحوكمة – تكشف جميعها أن السيادة الرقمية مفهوم متعدد الأوجه يتشكل وفق التاريخ السياسي والمصالح الاقتصادية والاعتبارات الأمنية لكل دولة.

على هذه الخلفية، برزت التجربة الأردنية بوصفها مسارًا واقعيًا يجمع بين البناء المؤسسي) المركز الوطني للأمن السيبراني و(JoCERT، والإطار التشريعي (الاستراتيجيات الوطنية وقانون الجرائم الإلكترونية)، والبعد الأكاديمي الذي يراكم رأس المال البشري. غير أنّ ما تحقق – على أهميته – يظل قاعدة انطلاق لا خط نهاية، ما لم يُستكمل بمنظومة قرار سيادي استباقية تتحوّل فيها البيانات إلى معرفة، والمعرفة إلى قرار، والقرار إلى تنفيذ يُقاس بمؤشرات أداء واضحة.

قدّم الفصل خارطة طريق عملية من تسعين يومًا بثلاث مراحل: تأسيس وتحليل، ثم بناء وتمكين، فتشغيل واستدامة. جوهر هذه الخارطة ليس ضغط الزمن بقدر ما هو توحيد المسار :فريق وطني متعدد التخصصات، خريطة مخاطر وطنية، غرفة قرار تعمل على مدار الساعة، مركز إنذار مبكر، سياسات قطاعية متمايزة، تمارين محاكاة واقعية، وميثاق سيادي رقمي يرسّخ الهوية ويضبط الشراكات.

وتبيّن أن عناصر النجاح ليست تقنية فحسب، بل سياسية وبشرية ومؤسسية : إرادة سياسية عليا تُعطي الأمن السيبراني أولوية استراتيجية؛ استثمار جاد في التعليم والبحث والتدريب ليصبح الإنسان خط الدفاع الأول؛ شراكات إقليمية ودولية تُنقل المعرفة دون التنازل عن القرار الوطني؛ ومؤشرات أداء (KPIs) تُخرج الخطاب من عمومياته إلى أرقام قابلة للقياس والتحسين المستمر.

بهذه الرؤية، يتجاوز الأردن ثنائية "الاستهلاك/ التبعية" نحو موقع المبادِر وصانع الرؤية إقليميًا، مستندًا إلى موقع جغرافي رابط، وتنوع اجتماعي محفّز للابتكار، ورأسمال بشري شاب. وعندما تتكامل هذه الموارد مع إطار مؤسسي مرن وقدرة تنفيذية منضبطة، تصبح السيادة الرقمية ممكنة وفاعلة، لا شعارًا ولا ترفًا.

لا يدّعي هذا الفصل اكتمال الصورة، بل يقترح جدول أعمال مفتوحًا للتطوير: تحديث دوري للأطر القانونية بما يوازن بين الأمن والحقوق؛ تعميق الربط اللحظي بين القطاعات الحيوية وغرفة القرار؛ تعميم ثقافة الأمن السيبراني مجتمعيًا؛ وفتح مسارات تمويل وابتكار تُحوّل الجامعات والمختبرات إلى محرّكات حلول وطنية قابلة للتصدير.

أن القرار السيبراني ليس مجرد تقنية بل أفق سيادي :يَجعل الدولة قادرة على صون فضائها الرقمي، وعلى إعادة تعريف استقلالها في نظام عالمي تُدار قوته عبر البيانات والخوارزميات. وإذا كان العالم يعيد رسم خرائط النفوذ في الفضاءات غير المرئية، فإن الأردن يمتلك اليوم – بما تحقق وما يمكن تحقيقه – مقوّمات الانتقال من الهشاشة إلى القوة، ومن الاستجابة إلى الاستباق .تلك هي دعوة الفصل وعودته: أن نعامل السيادة الرقمية كسياسة دولة لا مشروع جهة، وكقدرة مُقاسة لا سردية مُعلّقة، وكطريقٍ يبدأ بخطوة محسوبة... ثم يمضي بثبات.

# الفصل التاسع

# دروس مستخلصة من الميدان السيبراني

# مقدمة الفصل

في عالم تتسارع فيه الأحداث وتتكاثر فيه التهديدات الرقمية، لا يكفي أن نروي قصص النجاح أو نعرض النماذج المثالية للحماية. فالميدان السيبراني، مثل ساحة المعركة، يفيض بالدروس القاسية التي تُصاغ من خلال الفشل أكثر مما تُصاغ من خلال النجاح. إنّ كل حادثة اختراق، وكل انقطاع في البنية التحتية، وكل استغلال لثغرة أمنية، تحمل في طياتها عبرةً ثمينة :أن الأخطاء الصغيرة قد تتحوّل إلى كوارث وطنية إذا لم تُدرك في وقتها.

لقد أثبت التاريخ أن الهزائم ليست مجرد خسائر لحظية، بل علامات فارقة تُعيد صياغة وعي المؤسسات والدول. فعندما أصاب هجوم Stuxnet الأنظمة الصناعية الإيرانية عام 2010، لم يكن الأمر مجرد خلل تقني، بل صدمة كشفت للعالم أن الشيفرة يمكن أن تعادل في تأثيرها أقوى الأسلحة التقليدية. وعندما اجتاح WannaCryالمستشفيات البريطانية عام 2017، تبيّن أن الاعتماد على أنظمة تشغيل قديمة هو خطأ مؤسسي لا يقل خطورة عن غياب جيش في ساحة المعركة. أما SolarWinds (2020)فقد أظهر أن سلاسل التوريد الرقمية يمكن أن تتحوّل إلى أخطر أبواب الاختراق، حتى لأكبر القوى العالمية.

هذه الدروس لا تقتصر على القوى الكبرى؛ ففي بيئتنا العربية والأردنية على وجه الخصوص، واجهت بعض المؤسسات المالية والتعليمية والبلدية محاولات اختراق كان يمكن أن تتحوّل إلى أزمات واسعة لو لم يُتدارك الأمر. وغالبًا ما كان السبب واحدًا: إما ضعف في ثقافة الوعي الأمني، أو غياب سياسات استجابة واضحة، أو الاعتماد المفرط على حلول مستوردة دون مواءمة محلية.

إنّ هذا الفصل لا يقدِّم بوصفه سردًا للأخطاء فحسب، بل كـــ مرآة استراتيجية تساعد القارئ على إدراك أن السيادة الرقمية تُبنى على أساسين متكاملين: ما نفعله بشكل صحيح، وما نتجنّب الوقوع فيه من أخطاء. فمن خلال تصنيف وتحليل الأخطاء الشائعة عبر الفصول السابقة، سيجد القارئ هنا خريطة ذهنية واضحة تُرشده إلى ما ينبغي أن يُتجنَّب، بنفس القدر الذي يرشده الكتاب إلى ما ينبغي أن يُتَّبع.

ولعلّ أعظم ما في هذه الدروس أنها تكشف عن طبيعة التهديد السيبراني كظاهرة متكررة :الهجمات تختلف في أشكالها، لكن الأخطاء التي تستغلها تبقى متشابهة؛ من غياب التحديثات، إلى ضعف إدارة الهوية، إلى غياب التنسيق المؤسسي. وهذا يعني أن الوقاية ليست في ملاحقة كل تهديد جديد على حدة، بل في بناء منظومة قرار سيادي تستوعب الماضي والحاضر وتستشرف المستقبل.

إنّ الميدان السيبراني لا يرحم الغافلين، ولا يمنح فرصة ثانية لمن يستهين به. لذا، فإن هذا الفصل الختامي يأتي كجرس إنذار، وكخلاصة عملية، وكدعوة إلى أن ننظر إلى الأخطاء لا بوصفها وصمة عار، بل باعتبارها معلمًا على طريق التعلم والسيادة. فمن يتجاهل دروس الماضي، سيجد نفسه حتمًا يعيد إنتاج نفس الأخطاء، لكن بثمن أكبر وأشد وقعًا.

### 9.1 الأخطاء الشائعة في المفاهيم والأسس العلمية

إنّ أول الأخطاء وأكثرها خطورة هو حصر الأمن السيبراني في نطاق تقني ضيق .كثير من المؤسسات ما زالت تتعامل معه بوصفه "خدمة دعم فني"، تُسند إلى قسم تقنية المعلومات أو إلى فريق محدود من المهندسين. هذه النظرة الضيقة تُفقد

الأمن السيبراني معناه الاستراتيجي؛ فالهجوم لا يستهدف جهازًا أو برنامجًا، بل يهدد القدرة المؤسسية على الاستمرار واتخاذ القرار.

- **الخطأ الأول: تقزيم الأمن السيبراني إلى مسؤولية تقنية فقط.**

هذا يجعل القرارات الأمنية تفتقر إلى الغطاء الإداري والسياسي، فتُصبح ردود الأفعال بطيئة وغير منسقة. دراسات عديدة (NIST, 2020) تؤكد أن أعلى نسب الفشل في الاستجابة للحوادث وقعت في مؤسسات لم يكن فيها الأمن السيبراني جزءًا من هيكل القيادة العليا.

- **الخطأ الثاني: الاعتماد على أدوات تقليدية بمعزل عن التفكير الاستراتيجي.**

مكافحة الفيروسات والجدران النارية التقليدية لم تعد كافية أمام هجمات معقدة مثل Advanced Persistent Threats (APT)، التي تعتمد على التواجد الخفي طويل الأمد داخل الشبكات. هجوم APT29 على وزارات الخارجية الأوروبية دليل على أن المهاجمين لا يبحثون عن "اختراق سريع"، بل عن موطئ قدم طويل الأمد.

- **الخطأ الثالث: غياب الثقافة الأمنية المؤسسية.**

ما لم يُدمَج الوعي الأمني في جميع مستويات المؤسسة، فإن أقوى الأنظمة ستفشل أمام "خطأ بشري" بسيط، مثل فتح رابط خبيث أو مشاركة كلمة مرور. حادثة Target (2013) مثال واضح، حيث استُغلت ثغرة في حساب مقاول خارجي، وليس في النظام الداخلي المباشر.

يتبين هنا أن الأمن السيبراني ليس وظيفة تقنية، بل إطار سيادي متكامل يبدأ من الوعي الفردي وينتهي بالقرار المؤسسي.

## 9.2 الأخطاء الشائعة في السيادة الرقمية

في هذا المجال، الخلط بين الأمن المعلوماتي والسيادة الرقمية هو أخطر ما يواجه الدول:

- قد تمتلك الدولة سياسات صارمة لحماية البيانات، لكنها تفقد سيادتها إذا كانت تلك البيانات مخزنة في خوادم خارج حدودها، أو خاضعة لقوانين دول أخرى.
- الاعتماد على البنى التحتية الأجنبية يجعل القرار الوطني هشًّا؛ فإذا أوقفت شركة مزوّدة خدمةً أو فرضت دولة أجنبية قيودًا، يصبح القرار السيادي معطلاً.

**مثال عالمي:**

مشروع GAIA-X الأوروبي وُلد من إدراك الاتحاد الأوروبي لخطأ الاعتماد الكلي على شركات أميركية في إدارة السحابة .(Amazon, Microsoft, Google) السيادة الرقمية ليست حماية تقنية فقط، بل ضمان أن تبقى البيانات والخدمات تحت الإطار القانوني والسياسي الوطني.

**مثال محلي:**

في الأردن، خلال جائحة كورونا، لجأت معظم المؤسسات التعليمية إلى منصات أجنبية للتعليم عن بعد. رغم أنها وفرت الحلول التقنية، إلا أن هذا خلق اعتمادًا كاملًا على خوادم وقوانين غير وطنية، ما كشف عن فجوة في القرار السيادي الرقمي.

الدرس هنا أن السيادة الرقمية ليست شعارًا، بل هي امتلاك كامل لسلسلة القيمة الرقمية :من البنية التحتية إلى الخوارزميات إلى التشريعات.

### 9.3 الأخطاء الشائعة في البنية التحتية والهندسة السيبرانية

أحد أكثر الأخطاء شيوعًا هو التعامل مع البنية التحتية الأمنية كأنها "قطع متناثرة"، لا كشبكة متكاملة:

- عندما تُدار الشبكات بمعزل عن السحابة، أو تُترك الأنظمة القديمة بلا تحديث، فإن المهاجم يجد طريقًا عبر "أضعف حلقة."
- الاعتماد على "الشراء" بدل "التصميم السيبراني" يؤدي إلى حلول متضاربة.

**مثال عالمي:**

هجوم WannaCry (2017) شلّ المستشفيات البريطانية لأنه استغل ثغرات في أنظمة تشغيل قديمة (Windows XP) لم تُحدّث. المشكلة لم تكن في غياب الحلول، بل في ضعف إدارة التحديثات والمرونة المؤسسية.

**مثال محلي:**

بعض البنوك الأردنية واجهت في السنوات الأخيرة محاولات اختراق نتيجة ضعف الربط بين أنظمة الفروع والأنظمة المركزية، ما أبرز غياب "الهندسة السيبرانية الكاملة."

وهنا نتعلم ان البنية التحتية الأمنية يجب أن تُصمم وفق مبدأ Defense in Depth (الدفاع في العمق)، حيث لا يُترك أي نظام أو نقطة وصول دون حماية متكاملة.

### 9.4 الأخطاء الشائعة في تحليل الثغرات وإدارة المخاطر السيبرانية

إحدى أخطر المشكلات في هذا المجال هي التعامل مع تقييم الثغرات باعتباره **نشاطًا دوريًا روتينيًا**، بدل أن يكون جزءًا من دورة حياة مستمرة لإدارة المخاطر.

- **الخطأ الأول: الاكتفاء بالفحص الدوري دون خطط استجابة.** الفحص وحده لا يكفي إذا لم يُتبع بخطة إغلاق الثغرات. هجوم Equifax (2017)يُعتبر مثالًا شهيرًا؛ حيث كانت الثغرة معروفة وتم التحذير منها، لكن عدم الاستجابة السريعة أدى إلى تسريب بيانات 147 مليون شخص.

- **الخطأ الثاني: غياب التوثيق والتحليل بعد الحوادث.** كثير من المؤسسات تتعامل مع الهجوم على أنه حدث يجب تجاوزه بسرعة، دون تسجيل دروس مستفادة. النتيجة: تكرار الأخطاء نفسها. في دراسات الحوادث الأمنية بالشرق الأوسط(PwC, 2021) ، تبين أن ٪58 من المؤسسات لم تراجع قراراتها بعد الهجوم.

- **الخطأ الثالث: التركيز على التقنية وإهمال العنصر البشري.** الأخطاء البشرية أو الإهمال الداخلي مسؤولة عن أكثر من ثلث الحوادث (Verizon DBIR, 2020).تدريب الموظفين على الوعي الأمني لا يقل أهمية عن استخدام أدوات المسح مثل Nessusأو OpenVAS.

لاحظ ان إدارة المخاطر ليست مجرد فحص ثغرات، بل منهجية متكاملة تشمل التقييم، التوثيق، الاستجابة، والتحسين المستمر.

## 9.5 الأخطاء الشائعة في الذكاء الاصطناعي والتعلم الآلي في الدفاع السيبراني

مع دخول الذكاء الاصطناعي إلى ميدان الأمن، ظهرت أخطاء جديدة تتعلق بالتوقعات المبالغ فيها:

- **الخطأ الأول: الثقة المفرطة في النماذج.** الذكاء الاصطناعي يتعلم مما يُعطى له من بيانات، وإذا كانت البيانات ناقصة أو منحازة، فإن النتائج ستكون مضللة. تقارير (MIT, 2021) تشير إلى أن بعض أنظمة كشف التهديدات فشلت في اكتشاف هجمات صفرية (Zero-Day) لأنها لم تُدرَّب عليها.

- **الخطأ الثاني: الاعتماد الكامل على الأتمتة.** القرار الأمني يحتاج دومًا إلى إشراف بشري. في إحدى شركات الطاقة الأوروبية، عطّل نظام ذكي جزءًا من الشبكة لأنه "ظن" أن نشاطًا مشروعًا هو هجوم. هذا يوضح خطورة إقصاء العنصر البشري.

- **الخطأ الثالث: تجاهل التكلفة والجاهزية.** كثير من المؤسسات الصغيرة والمتوسطة تستثمر في أنظمة AI باهظة الثمن دون جاهزية بنية تحتية تدعمها. النتيجة هي حلول غير فعّالة أو غير مستدامة.

وهنا نجد ان الذكاء الاصطناعي قوة مضاعفة، لكنه ليس بديلًا عن العقل البشري الواعي ولا عن البنية التحتية الجيدة.

### 9.6 الأخطاء الشائعة في التعامل مع الهجمات السيبرانية الكبرى

أكبر خطأ هنا هو النظر إلى الهجمات كحوادث تقنية منعزلة عن سياقها السياسي والاقتصادي.

- **الخطأ الأول: إهمال الأبعاد الاستراتيجية.** هجوم Stuxnet (2010) لم يكن مجرد اختراق، بل عملية استراتيجية غيّرت ميزان القوى النووية. كذلك، SolarWinds (2020) كشف هشاشة سلاسل التوريد التي تعتمد عليها أقوى مؤسسات الدولة الأميركية.

- **الخطأ الثاني: ضعف التنسيق المؤسسي**. في هجوم NotPetya (2017)، تسببت القرارات المتفرقة وغير المنسقة في تضاعف الخسائر لتتجاوز 10 مليارات دولار عالميًا.
- **الخطأ الثالث: عدم تحويل الأزمات إلى فرص تعلم**. دول مثل إستونيا استفادت من الهجوم السيبراني الشامل عام 2007 لبناء واحدة من أقوى منظومات الدفاع الرقمي في العالم. بينما مؤسسات أخرى تكرّر الأخطاء نفسها لغياب الوعي التحليلي.

ان الهجمات السيبرانية الكبرى هي معارك استراتيجية يجب أن تُقرأ في سياقها الأوسع، لا مجرد أعطال تقنية.

### 9.7 الأخطاء الشائعة في هندسة القرار السيبراني

نقاط الضعف في هذا المجال مرتبطة غالبًا بالمنهجية:

- **الخطأ الأول: القرارات الارتجالية**. ما زالت بعض المؤسسات تستجيب للهجمات كما لو كانت "إطفاء حرائق"، دون الاعتماد على أطر منهجية مثل OODA Loop (Observe–Orient–Decide–Act)أو Cyber Kill Chain.
- **الخطأ الثاني: غياب قياس الأثر**. القرارات تُتخذ أحيانًا بلا مؤشرات أداء (KPIs)أو مراجعة لاحقة، مما يكرّس الفوضى. في تحليل لقطاع البنوك العربي(KPMG, 2022) ، تبيّن أن 45٪ من المؤسسات لم تقيّم أثر قراراتها الأمنية بعد الحوادث.

- **الخطأ الثالث: الفصل بين التحليل الفني والرؤية الاستراتيجية.** عندما يعمل الفنيون بمعزل عن صانعي القرار، تضيع المعلومات الدقيقة في مستويات البيروقراطية. النتيجة: قرارات متأخرة أو غير دقيقة.

الدرس المستخلص :هندسة القرار السيبراني هي علم + فن :إطار منهجي يُترجم المعلومة إلى قرار استباقي مدروس.

### 9.8 الأخطاء الشائعة في الحوكمة الرقمية وصناعة القرار

الاعتقاد أن "التحول الرقمي" مجرد إدخال التكنولوجيا في الإدارة، بينما هو في جوهره إعادة صياغة العلاقة بين المواطن، الدولة، والبيانات. مثل استيراد نماذج حوكمة أجنبية دون تكييفها للسياق المحلي، ما يجعلها غير قابلة للتطبيق.

**الخطأ الأول: اختزال التحول الرقمي في التكنولوجيا فقط.**

إدخال أنظمة إلكترونية دون تغيير في السياسات والثقافة المؤسسية يجعل الرقمنة سطحية وغير فعالة.

**الخطأ الثاني: استنساخ نماذج أجنبية دون تكييف.**

تبنّت بعض الدول لائحة GDPR الأوروبية دون جاهزية للبنية التحتية أو الثقافة القانونية المحلية، ما جعلها نصوصًا جميلة بلا تطبيق.

**الخطأ الثالث: غياب مؤشرات قياس واضحة.**

لا يمكن إدارة ما لا يُقاس. كثير من برامج الحوكمة الرقمية تفشل لأنها بلا معايير لقياس النجاح أو الأثر.

الدرس المستخلص :الحوكمة الرقمية ليست تقنية فقط، بل إطار سيادي لإدارة البيانات وصناعة القرار، يجب أن يُبنى محليًا مع الاستفادة من التجارب العالمية.

## خاتمة الفصل

يقول ســن تزو في *فن الحرب*" :*في قلب كل أزمة، تكمن فرصــة* ".وهذا ما يكشفه لنا الميدان السيبراني اليوم: أن التهديدات ليست فقط تحديات تهدد بقاءنا، بل أبوابًا لصياغة وعي جديد وسيادة رقمية أكثر رسوخًا. كل خطأ وقعنا فيه، أو وقعت فيه دول ومؤسسات من قبلنا، ليس نهاية الطريق، بل درسًا حيًا يجب أن نحمله معنا كعلامة إنذار، وكبذرة وعي تُثمر سيادة.

لقد أظهرت لنا كتب الحروب أن الانتصــار لا يكون دائمًا بالقوة الغاشــمة، بل بالذكاء، بالبصــيرة، وبالقدرة على قراءة الخصــم قبل أن يتحرك. وأظهرت لنا كتب التنمية الذاتية أن الإنســان، كالفرد وكالمجتمع، لا يتقدّم إلا عندما يتعلّم من عثراته، ويحوّل جراحه إلى قوة دافعة. أما المجالات السيبرانية الحديثة فقد كشفت أن أعظم الأخطاء هي تكرار ما كان معروفًا، وأن أعظم الانتصارات هي الاستفادة من كل خطأ لتحويله إلى دفاع أقوى وهندسة أذكى.

إنّ استعراض الأخطاء الشائعة لم يكن غايته التوبيخ ولا جلد الذات، بل تأسيس وعيٍ عميق بأن الســيادة الرقمية ليســت مجرد أدوات أو تقنيات، بل ثقافة قرار، تُبنى بالوعي مثلما تُبنى بالأنظمة. فالهجوم قد يبدأ من سـطر كود، لكنه في جوهره يسـتغل فجوة بشرية أو مؤسسية أو تشريعية. وهنا يظهر جوهر المعركة: من لا يعرف أخطاءه سيُهزم بها، ومن يعرفها ويحوّلها إلى دروس سيخرج منها أكثر قوة.

وكما قال كلاوزفيتز" :*الحرب هي استمرار للسياسة بوسائل أخرى* ".يمكننا أن نقول اليوم :الهجوم السـيبراني هو اسـتمرار للصـراع بوسـائل رقمية، تتجاوز الحدود المادية لتطال جوهر السيادة ذاته. وكما أكد مكيافيلي" :*الأمير الحكيم هو الذي يبني*

*على ما يملك، لا على ما يستعيره* ".فإن الدولة أو المؤسسة التي لا تبني بنيتها الرقمية الذاتية ستظل أسيرة قرار خارجي مهما بلغت قوتها الظاهرة.

لكن هذا ليس قدرًا محتومًا. لقد أثبتت التجارب العالمية أن المؤسسات التي تعلّمت من إخفاقاتها هي التي صنعت سيادتها لاحقًا .إستونيا مثلًا، بعد هجوم 2007 الذي شلّ خدماتها، لم تنكسر، بل جعلت من التجربة نقطة انطلاق لتصبح من أكثر الدول تقدمًا في الدفاع الرقمي. وهذا عين ما تقوله فلسفة التنمية الذاتية: إن الأزمة ليست نهاية، بل بداية جديدة لمن يحسن استثمارها.

وعليه، فإننا أمام حقيقة واضحة:

- الأخطاء ستحدث، لكن الوعي بها يحوّلها إلى أسلحة دفاعية.
- التهديدات ستبقى، لكن تحويلها إلى فرص هو ما يصنع السيادة.
- القرارات قد تخطئ، لكن هندستها على أسس علمية يعيدها إلى مسارها الصحيح.

إنّ السيادة الرقمية لا تُصان بالصدفة، بل بالوعي المتجدد، بالقرارات المدروسة، وبالمثابرة المستمرة على التعلم من الميدان. وكما أن القادة في الحروب القديمة كانوا يجمعون بين الحذر والجرأة، فإن القادة الرقميين اليوم يجب أن يجمعوا بين التحليل العلمي والخيال الاستباقي، بين الانضباط المؤسسي والقدرة على التغيير.

هذه الخاتمة ليست إغلاقًا للكتاب فحسب، بل بداية لفصل جديد في وعي القارئ: أن يكون فاعلًا، لا متفرجًا؛ مبادرًا، لا متأخرًا؛ صانعًا للقرار، لا متلقيًا له. إنّ

الأمن السيبراني المتقدم ليس ترفًا، بل قدرًا سياديًا، ومن يتقنه يملك مستقبله، ومن يهمله سيجد نفسه محكومًا بقرارات لم يشارك في صياغتها.

فلنعتبر هذه الدروس إذن دعوة للوعي، وصوتًا للعقل، وبوصلة للقرار. وكما قال سن تزو" :*الانتصار الأعظم هو أن تهزم عدوك دون قتال* ".فإن الانتصار الأعظم في ميدان السيبرانية هو أن نبني سيادتنا بحيث لا يجد الخصم منفذًا، ولا يملك سوى الاعتراف بقوتنا ووعينا.

# خاتمة الكتاب

لقد كشفنا أن السيادة الرقمية ليست خيارًا تقنيًا، بل مشروع وطني شامل، يحدد قدرة الدول على حماية هويتها، وصون قرارها، وتحصين مستقبلها في عالم بلا حدود. ومن هنا، لا يقتصر دور هذا الكتاب على التنظير أو السرد، بل يسعى ليكون أداة عملية لإعادة صياغة السياسات العامة، وبناء قدرات مؤسسية قادرة على حماية الأوطان من التبعية الرقمية والهيمنة التقنية.

أما على المستوى العربي والإقليمي، فإن الرسالة أبعد من الحدود القُطرية. هذا الكتاب دعوة مفتوحة إلى بناء تحالفات سيبرانية عربية، قادرة على صياغة أطر ومعايير مشتركة، تُوازن بين الانفتاح على العالم وحماية الخصوصية الثقافية والسيادة الوطنية. فكما لا تُبنى الجيوش منفردة، لا تُبنى المنظومات السيبرانية بمعزل عن شراكات إقليمية ودولية واعية.

إن القيمة الكبرى لهذا العمل تكمن في كونه جسرًا بين الفكر والسياسة والتقنية: فهو يقدّم أدوات تشغيلية وخططًا واقعية يمكن تبنيها اليوم، ويزرع في الوقت ذاته بذور رؤية مستقبلية تتجاوز اللحظة الراهنة، نحو فضاء عربي سيبراني آمن، مرن، وفاعل.

ولذلك، نختم برسالة واضحة:

إنّ السيادة الرقمية لم تعُد رفاهية فكرية، بل شرطًا للبقاء في عالم يُعاد تشكيله بالكود أكثر مما يُعاد بالقوة الصلبة.

وهذا الكتاب، بكل ما يحمله من رؤى وأدوات، ليس نهاية الطريق، بل بداية لرحلةٍ طويلة، نخطوها معًا نحو مستقبل تُصاغ فيه قراراتنا الرقمية بأيدينا، وتُبنى فيه نهضتنا على استقلالية فكرية وتقنية تُعبّر عنّا وتحمينا.

**وفي نهاية هذا الكتاب......**

وفي نهاية هذا الكتاب، ندرك أن السيادة الرقمية ليست فصلًا من فصول الأمن السيبراني، بل هي جوهر الإدارة الحديثة في عصرٍ يُعاد فيه تعريف القوة والشرعية من خلال البيانات والخوارزميات. فكما أنّ علم الإدارة يعلّمنا أن القرارات تُصاغ عبر التخطيط، التنظيم، القيادة، والرقابة، فإن الميدان السيبراني يُضيف إليها بعدًا جديدًا : الاستباقية، حيث يصبح التنبؤ بالتهديد شرطًا للنجاة.

لقد بيّن لنا علم الإدارة أنّ جوهر القيادة يكمن في القدرة على التخطيط والتنظيم والتوجيه والرقابة. غير أن الميدان السيبراني أضاف بعدًا جديدًا :الاستباقية .فالزمن لم يعد يسمح بانتظار الهجوم، بل بقراءته قبل وقوعه. وهنا يلتقي علم الإدارة مع استراتيجيات الحرب القديمة: حين قال سن تزو إن "أعظم الانتصارات هي التي تتحقق دون قتال"، فإنه كان يصف ما نحتاجه اليوم في فضاء السيبرانية؛ أن نهزم التهديد قبل أن يولد.

ومن خلال استراتيجيات صنع القرار، ندرك أن الفعل العشوائي أخطر من التهديد ذاته. فالنماذج مثل OODA Loop وKill Chain وFAIR تعلمنا أن القرار عملية مستمرة من الملاحظة، التحليل، التوجيه، ثم الحسم. لكن أعظم القرارات هي تلك التي لا تكتفي بالتحليل، بل تضيف البصيرة الإنسانية التي تجعل الأرقام معنى، والتقارير وعيًا.

كما علمتنا الحياة أن الأزمات ليست نهايات، بل بدايات متنكرة. وأنّ المحن ليست قيودًا، بل مختبرات لصناعة القوة. وهذا عين ما نراه في الميدان السيبراني: كل هجوم، كل ثغرة، كل إخفاق، هو رسالة تقول لنا إن هناك شيئًا يجب أن يُفهم، يُعالج،

ويُبنى عليه. من يتجاهل الدرس يكرر الخطأ، ومن يتعلم يصبح أكثر صلابة، كما يصبح الفرد أقوى بعد أزماته.

وفي الوقت نفسه، تذكّرنا كتب الحروب أن النصر لا يُبنى بالقوة وحدها، بل بالدهاء، بالقدرة على الإخفاء، وبالمفاجأة. قال مكيافيلي" :الأمير الحكيم هو الذي يبني على ما يملك، لا على ما يستعيره ".وهذا درس سيادي بامتياز: فلا دولة تستطيع أن تملك قرارها إن كانت تعتمد في خوارزمياتها وبناها التحتية على الغير. وقال كلاوزفيتز" :الحرب هي استمرار للسياسة بوسائل أخرى ".ونحن نقول :الأمن السيبراني هو استمرار للسيادة بوسائل رقمية.

إنّ خلاصات هذه الحقول كلها، من الإدارة إلى الحرب، ومن التنمية إلى السيبرانية، تتقاطع في نقطة واحدة:

- أن الوعي بالأخطاء هو نصف المعركة.
- وأن القدرة على التعلم والتحول هي مفتاح القيادة.
- وأن القرار السيادي ليس خيارًا، بل ضرورة وجودية تضمن الاستقلال والاستمرار.

وفي نهاية هذا الكتاب، نعلن أن السيادة الرقمية ليست رفاهية فكرية، بل إدارة عليا للمستقبل .هي علم يُبنى على الأرقام، وحكمة تستلهم من التاريخ، وروح تتغذى من الأزمات، وأداة تُصاغ بالقرار الواعي.

إنها نداء لكل دولة ومؤسسة وفرد:

- لا تترك قرارك يُصاغ بيد غيرك.

- لا تجعل بياناتك تُدار خارج سيادتك.
- ولا تنتظر أن تعلّمك الأزمة ما كان يمكنك أن تستبقه بالوعي والمعرفة.

فالسيادة لا تُمنح، بل تُنتزع بالعلم. والأمن لا يُصان بالصدفة، بل يُبنى بالقرار. والمستقبل لا يُنتظر، بل يُصاغ بأيدٍ تعرف أن المعرفة قوة، وأن القرار وعي، وأنّ الوعي سيادة.

# المراجع

1. Boin, A., & Lodge, M. (2021). Governing the crisis: Designing resilient decision-making systems in cyberspace. Governance, 34(4), 789–807. https://doi.org/10.1111/gove.12602
2. Boyd, J. (1996). The essence of winning and losing (OODA Loop briefing). Unpublished manuscript.
3. Carr, N. (2010). The shallows: What the Internet is doing to our brains. W. W. Norton & Company.
4. FireEye. (2021). Annual threat report. FireEye, Inc.
5. Gartner. (2021). Adaptive security architecture and trends in cybersecurity. Gartner Research.
6. Gladwell, M. (2005). Blink: The power of thinking without thinking. Little, Brown and Company.
7. Helbing, D. (2019). Towards digital enlightenment: Essays on the dark and light sides of the digital revolution. Springer.
8. Hubbard, D., & Seiersen, R. (2020). How to measure anything in cybersecurity risk. Wiley.
9. International Data Corporation (IDC). (2023). DataSphere forecast report. IDC.
10. International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. ISO.
11. International Organization for Standardization. (2014). ISO/IEC 27036:2014 Information technology – Security techniques – Information security for supplier relationships. ISO.
12. International Organization for Standardization. (2015). ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO.
13. International Organization for Standardization. (2018). ISO/IEC 30141:2018 Internet of Things (IoT) – Reference architecture. ISO.
14. Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
15. Keeney, R. (2020). Value-focused thinking: A path to creative decision making. Harvard University Press.
16. Kindervag, J. (2010). Zero Trust model. Forrester Research.
17. Klimburg, A. (2020). The darkening web: The war for cyberspace. Penguin Books.
18. Lee, K. F. (2018). AI superpowers: China, Silicon Valley, and the new world order. Houghton Mifflin Harcourt.
19. Libicki, M. (2021). Cyberspace in peace and war. Naval Institute Press.

20. Lockheed Martin. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin Corporation.
21. Machiavelli, N. (1995). The prince (Original work published 1532). University of Chicago Press.
22. Maurer, T. (2022). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
23. National Institute of Standards and Technology (NIST). (2015). Guide to industrial control systems (ICS) security (SP 800-82 Rev. 2). U.S. Department of Commerce.
24. National Institute of Standards and Technology (NIST). (2018). Cybersecurity framework. U.S. Department of Commerce.
25. National Institute of Standards and Technology (NIST). (2020). Zero Trust architecture (SP 800-207). U.S. Department of Commerce.
26. Nye, J. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
27. Ponemon Institute. (2022). Cost of a data breach report. IBM Security & Ponemon Institute.
28. Russell, S., & Norvig, P. (2020). Artificial intelligence: A modern approach (4th ed.). Pearson.
29. Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.
30. Simon, H. (1977). The new science of management decision. Prentice Hall.
31. Sun Tzu. (2005). The art of war (Trans.). Barnes & Noble Classics.
32. UNESCO. (2023). UNESCO report on AI and digital governance. UNESCO Publishing.
33. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
34. Wikipedia. (2024). Digital sovereignty. In Wikipedia, The Free Encyclopedia. Retrieved September 20, 2024, from https://en.wikipedia.org/wiki/Digital_sovereignty
35. Wikipedia. (2025). Cybersecurity. In Wikipedia, The Free Encyclopedia. Retrieved January 5, 2025, from https://en.wikipedia.org/wiki/Cybersecurity

# السيادة الرقمية

## وهندسة القرار

## في الأمن السيبراني المتقدم

لقد تغيّر ميدان القوة. لم تعد السيادة تُقاس بمدى امتداد الأرض، بل بمدى السيطرة على البيانات. لم يعد السلاح في البر والجو والبحر، بل في كودٍ رقمي ينساب في شبكاتك، يغيّر الأولويات دون أن تدري. إنّها "حروب بلا دماء"، لكنها أشد فتكًا لأنها تزرع الهزيمة في وعي المجتمع قبل أن تُحدث الدمار في بنيته التحتية.

يقدّم هذا الكتاب دراسة معمقة في ميدان السيادة الرقمية وهندسة القرار ضمن سياق الأمن السيبراني، جامعًا بين التحليل النظري الرصين والتطبيقات العملية المعاصرة. ويتناول الأطر المفاهيمية والسياسات الاستراتيجية التي تؤسس لحماية فعّالة للفضاء الرقمي الوطني، مع إضاءة خاصة على دور هندسة القرار بوصفها أداة فكرية وتنفيذية لتحويل البيانات إلى قرارات سيادية متزنة.

هذا الكتاب أداة للتنفيذ لا نصًا للقراءة فقط. نلتزم بدعم التطبيق تدريبًا واستشارةً وإعدادًا للقوالب التشغيلية وقياسًا للأثر، وتحديث المنهجية بما يوافق الخصوصية ويحفظ الحقوقوسيادة القانون.

دار صفاء للطباعة والنشر والتوزيع
المملكة الأردنية الهاشمية - عمّان - شارع الملك حسين
مجمع الفحيص التجاري - هاتف : 4611169 6 962+
تلفاكس: 4612190 6 962+ - ص.ب 922762 عمّان 11192 الأردن
safa@darsafa.info - safa@darsafa1.net - safa@darsafa.net